Ministerie van Economische Zaken

V E R S L A G

RVICTO 26
Informatiebeveiligingsdiensten

Marktraadpleging

Inzake de aanbesteding Resultaatverplichte ICT-opdrachten 2026 (RVICTO 26) op het gebied van Informatiebeveiliging ten behoeve van diverse Ministeries en hun onderdelen, alsmede enkele ZBO's.

TenderNed-kenmerk : TN 534872
IUC-registratienummer : 202409001
Datum : 30 september 2025

RVICTO 2026 – MARKTRAADPLEGING - VERSLAG

1 Inleiding

Voor u ligt het verslag van de marktraadpleging in het kader van Resultaatverplichte ICT-opdrachten 2026 (RVICTO) voor Informatiebeveiligingsdiensten, uitgevraagd door inkoopcategorie ICT-professionals Rijk, uitgevoegd door het Inkoop Uitvoering Centrum van het ministerie van Economische Zaken (IUC-EZ).

De aanleiding en achtergronden zijn beschreven in het Marktconsultatiedocument van 25 juli 2025, zoals gepubliceerd via TenderNed op 30 juni 2025, als ook in tweede versie op 10 juli 2025.

Wij zijn verheugd met de zeer waardevolle 24 ontvangen reacties (23 van potentiële inschrijvers en 1 van het Centrum voor Criminaliteitspreventie en Veiligheid-CCV). Grote dank gaat uit naar de partijen die hun tijd en moeite hebben gestopt in het geven van hun feedback. Onder de experts is de algemene indruk er één van een mooie opbrengst!

BELANGRIJK: dit verslag is een samenvatting van de strekking van de ontvangen reacties per gestelde vraag. In dit verslag zijn geen conclusies, reacties of overwegingen dezerzijds of andere gevolgtrekkingen voor het hierop volgende proces van aanbesteden. De opbrengst van deze marktconsultatie en de beelden daarop van de experts worden eerst met de deelnemers afgestemd en een en ander zal zijn uiting vinden in de aanbestedingsstukken. Er komt derhalve geen separaat document als reactie op de ontvangen reacties. Dit nu voorliggende verslag is het publieke sluitstuk van deze marktconsultatie.

2 Procedure

- Op 30 juni 2025 is het Marktconsultatiedocument met als bijlage bijlagen gepubliceerd.
- Hierop zijn 51 vragen binnengekomen, die op 17 juli 2025 met publicatie op TenderNed geanonimiseerd zijn beantwoord.
- Op 25 augustus 2025 hebben in totaal 23 marktpartijen hun reacties c.a. antwoorden op onze vragen aangeleverd.
- Op 30 september 2025 is het verslag van de marktraadpleging gedeeld met de respondenten.
- Op 7 oktober 2025 is het verslag zonder bezwaren vanuit respondenten op TenderNed gepubliceerd.

In totaal hebben 45 ondernemingen zich als “geïnteresseerd” aangemeld via TenderNed, als ook 1 partij na de sluitingsdatum.

3 Vragen marktraadpleging

Nummering
De nummering van de vragen is onveranderd die als in het Marktconsultatiedocument en de ontvangen reacties.

Percentages
Bij de nummering zie u een percentage staan. Dit percentage geeft en indicatie (want sterk afgerond) van het aantal ontvangen antwoorden, waarbij 100% = zonder partijen die op

onderdelen hebben aangegeven en/of laten zien dat een bepaald onderdeel niet van hun gading is. Het deel 'Algemeen' is door 23 partijen ingevuld: 100% = 23; Het deel 'Pentesten' is door 20 partijen ingevuld: 100% = 20; Het deel 'Red Teaming' is door 18 partijen ingevuld: 100% = 18; Het deel 'SOC-diensten' is door 16 partijen ingevuld: 100% = 16; Het deel "Overige IB-diensten' is in wisselend aantal per subonderdeel ingevuld, zodat 100% = 11 tot 22.
Met de percentages zelf wordt verder niets gedaan. Het geeft enkel wat beeld representativiteit van het aantal ontvangen antwoorden.

ALGEMEEN

A1 – [100%] Wat vindt u van de voorgenomen verdeling in onderwerpen en de daarin omschreven scope?

Over het algemeen vinden respondenten de onderverdeling van de scope logisch en herkenbaar is. De huidige segmentatie sluit aan bij hoe markten zijn ingericht op basis van expertise. Het deel "Overige IB-diensten" heeft niettemin nadere uitwerking nodig. Dit deel bundelt uiteenlopende diensten die elk hun eigen randvoorwaarden, kwaliteitscriteria als contractvorm kennen. Advies: verdere en duidelijke opsplitsing.

Ter overweging:

- Expliciet borgen van de samenhang tussen detectie, respons en herstel.
- Aanvullende diensten:
    - Centraal log- en data lake-beheer voor opslag, retentie, toegangsbeheer en normalisatie van securitydata.
    - Cloudbeheer- en integratiediensten, waaronder API-koppelingen en licentieconfiguratie, die essentieel zijn voor snelle implementatie en operationele effectiviteit.
    - Koppeling van SOC/VOC-resultaten aan GRC-processen en risicoregisters zodat technische bevindingen direct doorwerken in strategische besluitvorming.
- Bij pentesten ontbreekt broncodeonderzoek gericht op security.
- Er is dienstverlening gerelateerd aan Identity & Access-management gevraagd. De ervaring leert dat daadwerkelijke implementatie veelal in een zelfstandige aanbestedingen in de markt gezet worden. Voorbereidende werkzaamheden (onderzoeken Programma van Eisen, definitie scenario's e.d.) zijn nu niet benoemd in de definities van de percelen. Deze past het beste bij Overige IB-diensten. Idem voor security architectuur.
- Cloud security-gerelateerde dienstverlening, voor zover het gaat over het reviewen van de inrichting van een Cloud op het gebied van security, is specifieke dienstverlening vaak onder Pentestdienstverlening wordt geplaatst.
- Governance, Risk en Compliance-adviesdiensten niet scharen onder "Overige IB-diensten", maar als zelfstandig deel contracteren.
- SOC-dienstverlening voor IT-SOC en OT-SOC apart van elkaar uitvragen.

A2 – [100%] Ontbreken er naar uw beeld nog diensten in de genoemde onderwerpen? Zo ja, welke?

De meeste respondenten vinden dat de huidige onderwerpen goed aansluiten bij de gevraagde dienstverlening, maar signaleren een aantal hiaten en hebben behoefte aan

verduidelijking. Er wordt gepleit voor een bredere en explicietere dekking van het strategische domein en opkomende technologieën, met name AI.

Aanvullingen:
- Governance, Risk en Compliance (GRC) en beleidsadvisering
    - Information Security Management Systeem (ISMS)
    - Beleidsontwikkeling en strategievorming
    - Compliance assessments
    - Assurance-gerelateerde opdrachten zoals ISAE 3000/3402, SOC2 en DigiD ICT-beveiligingsaudits
- Ondersteuning bij Identity & Access Management (IAM)
- AI en innovatiegerichte beveiligingsdiensten
- Cloud security en cloud configuratie-audits
- Security by Design / DevSecOps-ondersteuning / Secure Development
    - Secure code reviews
    - CI/CD pipeline-beveiliging
    - Integratie van security in ontwikkelcycli
- Privacyadvies zoals DPIA's, BIO-assessments, NIS2-audits en maturity scans
- Supply chain security: Risicobeoordeling in de keten & vendor risk management
- OT-dienstverlening
- Business Continuity & Crisisvoorbereiding
- Securityarchitectuur en ontwerpbeoordelingen

Aandachtpunten:
- Het deel "Overige IB-diensten" is nu te breed en ongedifferentieerd. Hierdoor is het voor gespecialiseerde partijen lastiger om aan te bieden.
- De huidige scope is sterk operationeel ingevuld, terwijl strategisch advies en de samenhang tussen beleid, governance en technologie, cruciaal is voor succesvolle invulling.
- De dienstverlening zou ook kennisoverdracht en versterking van de interne capaciteit moeten omvatten.
- Innovatie speelt momenteel nauwelijks een rol. Een aantal partijen zijn niettemin van mening dat innovatie een gunningscriterium moet zijn, omdat het essentieel is voor de toekomstbestendigheid van dienstverlening.
- Hoewel er veel aanvullingen zijn voorgesteld, zijn er ook enkele respondenten die aangeven dat de gegeven scope wel volledig is.

A3 – [100%] Wat is naar uw mening een gebalanceerd aantal partijen bij een raamovereenkomst voor een onderwerp en hoe komt dat aantal tegemoet aan de gezochte waarden voor opdrachtgever en de te bieden waarden door de opdrachtnemer?
Zekerheidshalve: er wordt uiteraard niet gevraagd om een antwoord voor onderwerpen die niet van uw gading zijn. Ook: als bij een onderwerp deze vraag ook specifiek wordt gesteld, kunt u uw reactie daar geven en hier weglaten.

Het merendeel van de respondenten noemt aantallen met een bandbreedte 3 - 5. Met een dergelijke spreiding is er voldoende balans tussen:
- Concurrentie & innovatie
- Leveringszekerheid
- Kwaliteitsborging
- Praktische uitvoerbaarheid

Een aantal respondenten stelt aantallen afhankelijk van het betreffende deel. Met name bij "Overige IB-diensten" is meer diversiteit in aantallen, dan wel vindt men het lastig een aantal te geven voor de veelsoortige dienstverlening in dit deel.

A4 – [100%] In de raamovereenkomsten zullen diverse deelnemers afnemen. Hoe is het risico te mitigeren dat de vraag voor u te groot wordt om te kunnen leveren? Waar moeten wij rekening mee houden? Welke voorwaarden zijn voor onze deelnemers relevant? *Zekerheidshalve: er wordt uiteraard niet gevraagd om een antwoord voor onderwerpen die niet van uw gading zijn.*

Over het algemeen wordt het risico onderkent dat de vraag vanuit meerdere deelnemers op piekmomenten groter kan zijn dan verwacht of de levercapaciteit toelaat. Als antwoord wordt gegeven dat marktpartijen over schaalbare modellen, brede expertise en ruimte (internationale) capaciteit beschikken. Daarmee denkt men dat het risico, binnen randvoorwaarden, beheersbaar is. De belangrijkste maatregelen om dit risico te beheersen:

- Capaciteitsplanning, voorspelbaarheid en gecommitteerde afname
- Heldere scope en realistische opdrachten
- Evenwichtige verdeling van opdrachten
- Schaalbare en redundante leveringsmodellen
- Samenwerking, afstemming en [centrale] coördinatie
- Hanteren van een fair use policy / afnamegarantie / recht om opdrachten te weigeren bij capaciteitsdruk

<u>Aandachtspunten:</u>

- Werklast en inefficiënte van regelmatige minicompetities. Alternatief: vooraf gedefinieerde verdeling of automatische rotatie
- Overvragen en achterblijvende vragen brengen het risico dat een opdrachtnemer investeringen niet rendabel krijgt. Voorstel: gegarandeerde volumes of afnameverplichtingen, vooral voor grotere opdrachten.
- Schaalbaarheid, automatiseringsgraad en bewezen leveringscapaciteit zou onderdeel van de selectie moeten zijn.
- Denk aan standaardiseren, zodat een detectie bij één deelnemer direct vergeleken kan worden of in de monitoring van andere deelnemers opgenomen kan worden.
- Overweeg fase- of prioriteitslevering mogelijk te maken wanneer nodig in scenario's met hoge vraag
- Zorg voor minimale doorlooptijden en duidelijke beschrijving van projectresultaten bij NOK en afroeping zodat de opdrachtnemer middelen effectief kan inzetten.

A5 – [100%] Bent u geïnteresseerd om in te schrijven op een of meer onderwerpen van de voorgenomen aanbesteding? Zo ja, welke onderwerpen?

Respondenten geven overwegend aan geïnteresseerd te zijn om in te schrijven op (enkele van) de voorgenomen aanbesteding(en). Men kan een brede scope van informatiebeveiligingsdiensten leveren. De onderwerpen in volgorde van interesse om in te schrijven onder respondenten.

1) Penetratietesten [>80%]
2) Red Teaming
3) SOC-diensten
4) Incident Response
5) Thread Intelligence

6) Awareness-diensten
7) Forensisch onderzoek
8) Overige IB-diensten / IB-Consultancy [>60%]

Enkelen geven aan eerst bij de precieze perceelindeling en voorwaarden hun definitieve keuze kunnen maken. Voor Penetratietesten en Red Teaming geldt dat men overwegend in beide delen geïnteresseerd zijn.

We zien een dat een aantal partijen op alle onderwerpen willen inschrijven en andere partijen bewust kiezen voor een selectie van onderwerpen waar ze bewezen ervaring of schaalbare capaciteit hebben. Het aantal onderwerpen waarop een marktpartij wil inschrijven is een indicatie over de mate waarin een marktpartij een meer of minder gespecialiseerd aanbod levert. De opsomming hieronder is een weergave van aantal respondenten per aantal onderwerpen volgens opsomming hierover.

- 8 respondenten zijn geïnteresseerd in 8 onderwerpen
- 2 respondenten zijn geïnteresseerd in 7 onderwerpen
- 3 respondenten zijn geïnteresseerd in 6 onderwerpen
- 2 respondenten zijn geïnteresseerd in 5 onderwerpen
- 4 respondenten zijn geïnteresseerd in 4 onderwerpen
- 2 respondenten zijn geïnteresseerd in 2 onderwerpen.
- 2 respondenten zijn geïnteresseerd in 1 onderwerp.

De meest gespecialiseerde partijen richten zich op SOC-diensten, eventueel aangevuld met penetratietesten.

<u>Aandachtpunten:</u>

- Perceelindeling en clustering is doorslaggevend voor het daadwerkelijke besluit wel/niet in te schrijven.
- Enkele partijen vragen expliciet aandacht voor de gevolgen van ABRO en het verkrijgen van een ABRO-verklaring. Tevens wordt aan opdrachtgever meegegeven om per nadere overeenkomst te bepalen of ABRO van toepassing moet zijn om zo onnodige vertraging en kosten te voorkomen.
- De inzet van internationale resources is afhankelijk van de regelgeving en eisen in de aanbesteding (EER-landen; gegevenssoevereiniteit)

A6 – [100%] In hoeverre ziet u het effect van de ontwikkeling in de EU rond digitale autonomie/soevereiniteit in de komende tijd op uw producten en dienstverlening in relatie tot de onderhavig voorgenomen aanbestedingen?

Zorgen over afhankelijkheid van niet-Europese technologie worden herkent en erkent. De toenemende relevantie in beleid en praktijk en het belang worden breed onderschreven. De antwoorden lopen uiteen van partijen die stellen dat dit een grote uitdaging is tot partijen die stellen dat ze er klaar voor zijn en weinig problemen voorzien. Hierbij aangetekend dat men "autonomie/soevereiniteit" vanuit verschillende perspectieven benadert. Men kijkt naar de locatie waar dataverwerking plaatsvindt, of gaat uit van EU-jurisdictie, dan weer zien het breder zien als "in control zijn" over data en processen. Hoewel iedereen de ontwikkelingen rond soevereiniteit, is niet iedereen concreet over het effect op producten en dienstverlening. Het wordt gezien als een zeer complex vraagstuk.
Momenteel wordt door marktpartijen veel gebruik gemaakt van technologie vanuit de VS en Israël, met name op het gebied van SOC, ECR/XDR en Cloud. Echte Europese alternatieven acht men nog schaars en technisch/functioneel onvoldoende volwassen. 100% Europese

oplossingen is niet realistisch zonder in te boeten op kwaliteit, gebruikersgemak of interoperabiliteit, waarschijnlijk (voorlopig) wel duurder. Diverse aanbieders hebben hun infrastructuur, opslag en dienstverlening al wel ingericht binnen de EU/EER. Ook is er sprake van pro-actief hostingbeleid, open source oriëntatie en gebruik van leveranciers met Europese eigendomsstructuren.
Met name voor SOC-diensten wordt de impact van soevereiniteit als zeer groot en complex gezien. Voor andere diensten zoals pentesten, Incident Response, IB-consultancy en awareness-diensten is de impact minder tot beperkt: deze kunnen relatief eenvoudig binnen de EUR-kaders worden geleverd.
Er is overheidsbeleid dat digitale soevereiniteit nastreeft en gelijktijdig is de overheid op veel plaatsen zelf afhankelijk van niet-Europese diensten (Azure, AWS, etc.). Houdt daarom rekening met proportionele en wederkerige eisen en wees alert op schijnzekerheid en ongelijk speelveld. Soevereiniteit is immers niet gelijk aan veiligheid of kwaliteit: eisen rond soevereiniteit zijn soms symbolisch of politiek gedreven en leiden niet altijd tot meer veiligheid of leveringszekerheid

Opvallend:
- Enkele respondenten schrijven dat ze nauwelijks tot geen impact verwachten van de ontwikkelingen rond digitale autonomie/soevereiniteit. In de meeste gevallen wordt autonomie/soevereiniteit gekoppeld aan organisaties die in Europese handen zijn en dataverwerkingen die binnen de EER plaatsvinden.
- Er is een partij die stelt dat zij 100% gebruik maken van Europese technologie en/of open source.

Aanbevelingen:
- Maak eisen rond digitale autonomie expliciet, onderbouwd, meetbaar en realiseerbaar zijn. Benoem concreet waar ze betrekking op hebben: dataopslag; eigendom, locatie van personeel, juridische jurisdictie, technologiepartners, etc.
- Verschillende partijen pleiten voor realisme en consistentie. Als afnemers zelf afhankelijk zijn van een niet-EU dienst/Cloud/infra, moet dit worden meegewogen bij het stellen van eisen aan leveranciers.
- Gezien de huidige stand van zaken kan het verstandig zijn om eisen gefaseerd op te bouwen. Bijvoorbeeld: per direct: minimale eisen rond dataopslag (EER) en transparantie over de keten; later: voorkeur voor EU-gebouwde technologie of open source tooling; en in de toekomst: EU-only leveringsmodel en naleving van EUCS of nationale certificering.

A7 – [100%] Bij deelnemers is Nederlands, zowel schriftelijk als mondeling, de voertaal. In hoeverre verwacht u dat het eisen van de Nederlandse taal als voertaal een beperking is voor de gevraagde dienstverlening en mogelijk marktpartijen weerhoudt om in te schrijven?

Uit de reacties blijkt een genuanceerd beeld over het hanteren van Nederlands als voertaal binnen informatiebeveiligingsdiensten. De meerderheid van de marktpartijen kan in de huidige situatie hieraan voldoen, maar een goot deel benoemt ook potentiële beperkingen of risico's wanneer deze eis strikt en zonder uitzonderingen wordt gehanteerd. Nadelige gevolgen op prijs, beschikbaarheid en inzet van expertise. Er zijn ook partijen voor een dergelijke taal-eis het inschrijven op de aanbesteding in de weg staat.
Over het algemeen onderschrijft men het belang van begrijpelijke communicatie, juridische borging, en aansluiting op de context van Nederlandse overheden. Tegelijkertijd klinkt de waarschuwing voor de beperkende werking van een strikte taal-eis, met name voor specialistische of internationaal georiënteerde diensten zoals: SOC/SIEM, Red Teaming,

Threat Intelligence en Incident Response. Cybersecurity expertise is schaars, vooral Nederlandstalige experts in nichegebieden. Engels is nu eenmaal de standaardtaal in de internationale IT- en securitywereld en internationale of Engelstalige specialisten zijn vaak nodig zijn om hoogwaardige diensten te kunnen leveren. Een strikte taal-eis leidt mogelijk tot hogere kosten, verminderde kwaliteit of beperkte beschikbaarheid.
Een genuanceerde toepassing van de taal-eis zou werkbaar kunnen zijn, zoals het contractueel en klantgericht contact in het Nederlands, met technische uitvoering deels in het Engels; Generieke kwalificatie van rollen/functies (bv. alleen klantgerichte rollen vereisen Nederlands); Bepaalde rapportage verplicht in het Nederlands, uitvoering flexibel; eventueel werken met taalniveaus (bijv. C1/C2-niveau Nederlands als eis). Het taalvereiste kan ook per opdracht of dienst worden afgewogen (flexibele toepassing binnen een overkoepelend contract).
Terzijde: er wordt in vergelijkbare zin erop gewezen dat ook de VOG/integriteitsverklaringen kunnen zorgen voor een geografische kader/begrenzing.

3.1 Penetratietesten

Op het onderwerp Penetratietesten zijn in de marktraadpleging 15 vragen gesteld (P1 t/m P15). 19 Respondenten (bedrijven) hebben hierop hun antwoorden gegeven. Hiernaast heeft het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) een reactie gegeven op een deel van de vragen. Hieronder treft u na elke vraag een samenvatting van de ontvangen reacties aan.

P1 – [100%] Wat is uw bespiegeling rond het indelen van Penetratietesten en Red Teaming in afzonderlijke raamovereenkomsten en het beoogde effect daarmee op de markt en opdrachtgevers?

Over het algemeen acht men het splitsen van Pentesten en Red Teaming logisch en waardevol. Beiden kennen fundamentele verschillen in doel, aanpak, looptijd, expertise en risicoprofiel. Separatie draagt bij aan marktwerking omdat nichepartijen op hun specialisme kunnen inschrijven, stimuleert innovatie en meer evenwichtige concurrentie c.q. breder gebruik van het marktpotentieel. Tevens biedt het de situatie dat een Red-Team 'aan te vallen' omgevingen benaderen zonder voorkennis via andere opdrachten, zoals pentesten. Anderzijds is opgemerkt dat men wel de mogelijkheid wil hebben om op beide percelen in te kunnen schrijven. Eén respondent vindt samenvoegen van Pentesten en Red Teaming praktischer: het voorkomt bureaucratie en geeft volledig beeld. Het zijn vooral de grotere partijen die beide type diensten in hun portfolio hebben en de wat kleinere partijen die zich onderscheiden op één domein. Meerdere respondenten pleiten bij separate raamovereenkomsten voor coördinatie tussen beide om overlap of hiaten te voorkomen.

P2 – [100%] Is binnen het domein van pentesten een binnen de markt algemeen houvast van termen en typen van testen, waarmee de te leveren diensten houvast geboden kan worden, zodanig dat producten concreet in concurrentie kunnen worden uitgevraagd?

Er is brede consensus over het bestaan van algemeen erkende termen en kaders, zoals bijvoorbeeld: black box, grey box, white box en objecttypen zoals webapplicaties, infrastructuur, mobiele apps, API, cloud, IoT/OT. Qua referentiekaders kan houvast worden gevonden in breed gebruikte internationale standaarden, zoals: OWASP, PTES, NIST,

OSSTMM, CREST.Breed in de markt gebruikte referentiekaders dragen bij aandve vergelijkbaarheid, eenduidigheid en concurrentie op kwaliteit. Dit laat onverlet dat termen niet altijd uniform worden gebruikt met het risico op misinterpretatie en concurrentie bij time-boxed pentests kunnen leiden tot kwaliteitsverlies of onvergelijkbare voorstellen. Het advies is om eenduidige definities op te nemen in aanbestedingsdocumenten/intakeformulieren en/of te verwijzen naar bestaande bronnen (e.g. Cyberveilig Nederland, Rijksoverheids-keuzekaart securitytesten). Ook is geopperd de pentests via extra classificaties van elkaar te onderscheiden, zoals handmatig/geautomatiseerd, small/medium/large/special etc., zodat marktpartijen beter de verwachtingen van de opdrachtgevers kunnen inschatten.

P3 – [100%] Beoogd is te vereisen dat de pentesten worden uitgevoerd volgens de fasering van de Pentest Execution Standard (PTES) (http://www.pentest-standard.org/index.php/Main_Page) of, na acceptatie door de opdrachtgever, volgens de fasen van een vergelijkbare erkende industriestandaard. De belangrijkste overweging hierbij is de uniformiteit, volledigheid en passendheid van de PTES. Er geldt dus een uitgangspunt van PTES, tenzij... Hiernaast zijn combinaties met andere meer inhoudelijke standaarden toegestaan (o.a. OWASP, NIST e.a.). De vraag is of het standaard eisen van de fasering van PTES bezwaarlijk kan zijn en waarom c.q in welke gevallen? Zo ja, welke alternatieve standaard(en) voor de fasering van de pentest stelt u voor, in plaats van of naast de PTES?

PTES biedt zeker structuur, uniformiteit en transparantie, maart is ook deels verouderd (laatste update meer dan 10 jaar geleden) en kan te rigide zijn voor kleine/spoedopdrachten. Overwegend is met het eens dat de globale fasering in PTES gebruikt kan worden, maar er vooral risico's zijn bij toepassing van meer inhoudelijke zaken in de PTES. Er klinkt ook de waarschuwing dat een te rigide gebruik van de fasering van de PTES onwenselijk is en kostenverhogend kan werken. De aanbeveling is om, indien men dat wenst, PTES als basis te gebruiken en te combineren met andere actuele standaarden met de mogelijkheid tot afwijken waar dat passend is: flexibiliteit per opdracht wordt belangrijk geacht. Aanvullingen (c.q. alternatieven) voor het combineren met PTES zijn onder andere: OWASP, NIST, OSSTMM, CREST, MITRE ATT&CK, ISSAF, CIS-benchmarks.

P4 – [95%] Hoe kan worden ingespeeld op de verwachting van de opdrachtgever rond de in te zetten capaciteit voor een concrete opdracht in relatie tot wat de leveranciers bij inschrijving voor de ROK in het vooruitzicht hebben gesteld?

Een goed verwachtingsmanagement is essentieel, als ook een capaciteitsplanning, duidelijke intake per opdracht en realistische inschatting van volume/type opdrachten. Aanbevelingen in dat kader: bandbreedtes voor responstijden, (plannings)dashboards voor transparantie over de te verwachten vraag, vooraf vastgelegde randvoorwaarden in ROK om extra eisen in NOK te voorkomen, toepassing van sjablonen voor minicompetities. Eventuele capaciteitsgaranties door een opdrachtnemer zijn afhankelijk van duidelijkheid en voorspelbaarheid van opdrachtgevers over de opdrachten: het kan immers niet de bedoeling zijn dat leveranciers capaciteit vrijhouden zonder dat opdrachten volgen. Er zijn abonnementsvormen toe te passen met een vaste/minimale inzet per periode of om bij capaciteitspieken ruimte te krijgen om opdrachten te herverdelen over andere opdrachtnemers. Wel aandacht voor proportionaliteit: eisen moeten passen bij de omvang van de opdracht.

P5 – [95%] Wat is uw beeld bij het aantal partijen bij een raamovereenkomst? Relevante elementen zijn onder andere hoeveel pentesten u zou kunnen uitvoeren, naast wat u nu al doet (dus: wat u beschikbaar zou hebben voor deze ROK), dan wel het maximaal aantal

deelnemers dat u (gelijktijdig) kunt bedienen. Het is essentieel dat we beeld hebben van het absorptievermogen in de markt is en hoe daarop evenwichtig kan worden ingespeeld.
Overwegend acht men een bandbreedte van 3 tot 5 partijen als realistisch en werkbaar. Enkelen noemen een maximum variërend van 6 tot 11 partijen. Men ziet in de genoemde maxima voldoende keuze voor opdrachtgever, een beheersbaar contract, een eerlijke verdeling van het werk en het voorkomen van overbelasting van individuele leveranciers gezien de potentieel grote capaciteitsvraag. Wel wordt gewaarschuwd voor te veel partijen in een raamovereenkomst, wat versnippering, prijzenslag, gebrek aan voorspelbaarheid in de hand kan werken. Een evenwichtige marktabsorptie kan bij een (soms hoge/piek) capaciteitsvraag baat hebben bij een transparant verdeelmechanisme (e.g. roulatie of proportioneel naar scope, als alternatief op de standaard minicompetitie). Ook is de mogelijkheid geopperd om een beroep te kunnen doen op extra beschikbare capaciteit in het buitenland, dus niet te strikt vasthouden aan voertaal Nederlands. Ook is een schaalbaar model geopperd met twee lagen, waarbij de tweede laag (reserve)opdrachtnemers pas mag aanbieden zodra de eerste laag niet aan de vraag kan voldoen.
P6 – [100%] Wanneer is een offertetraject voor u zinvol om in een mini-competitie een aanbieding te doen? Denk hierbij aan overwegingen als: - Inkoop-inspanning vs. resultaat/rendement opdracht? - (Wanneer) past een afroepcontract onder de ROK? - Binnen welke kaders? - Hoe past een opdracht bij het aanbod? - Kans op de opdracht en het aantal opdrachtnemers in de ROK.
Er is consensus dat mini-competities alleen zinvol zijn bij grote of complexe opdrachten, niet voor een kleine/losse pentest. De gevraagde inspanning voor het uitbrengen van een offerte (meedoen aan mini-competities) moet in verhouding staan tot de opdrachtwaarde en terugverdienkans. Sommige respondenten noemen een concrete minimale waarde per opdracht, variërend van 15 tot 30 duizend euro. Een enkele respondent is in zijn geheel tegen mini-competities. Voor standaardopdrachten: is een brede voorkeur voor afroepconstructies met vaste prijzen/pakketten en/of een roulatiesysteem bij het verstrekken van opdrachten. Dit geeft minder administratie, betere voorspelbaarheid, en daarmee een betere capaciteitsplanning. Een verdeelsysteem van nadere opdrachten moet voldoende win-kans geven, beheerlasten beperken met uniforme/gestandaardiseerde aanvraagprocessen, duidelijke scope en tijdlijnen in aanvragen eisen, liefst meerdere testen bundelen in een opdracht, transparant zijn in de wijze van gunning en kwaliteit belangrijker stellen dan prijs.
P7 – [95%] Wat is uw beeld bij prijsmodaliteiten voor pentesten qua eenheid en voorspelbaarheid van totale kosten? We gaan uit van algemeen in markt gebruikelijke prijsmodaliteiten met daarin diverse vaste en verrekenbare elementen. Graag vernemen wij wat daarin voor-/nadelen kunnen zijn, met name ten aanzien van vaste en verrekenbare delen.
Vrijwel alle respondenten pleiten voor een hybride prijsmodel (vaste elementen + verrekenbare delen). Vaste prijzen zijn geschikt voor standaardopdrachten (b.v. black box webapplicatie, afgebakend op grootte of time boxed). Verrekenbare elementen kunnen worden toegepast bij maatwerk (b.v. uitvoering buiten kantooruren, gespecialiseerde testscenario's, PoC's, ketenanalyses), grotere scope, extra diepgang of hertesten. Met

betrekking tot de hertest: de definitie van een hertest moet duidelijk moet zijn, zodat het helder kan worden gescheiden als standaard onderdeel van een opdracht dan wel als extra te benoemen werk (alleen op eerder geconstateerde kwetsbaarheden, of wederom de gehele applicatie). Enkele respondenten adviseren een dagtarief of time box als uitgangspunt, gecombineerd met vaste prijsafspraken na intake. Hierbij de waarschuwing dat prijsdruk door mini-competities en (uitsluitend) vaste-prijs-afspraken de kwaliteit kan ondermijnen. Wellicht kan een tweeledig model baten: een vast tariefkader in de ROK en bandbreedtes per opdracht in de NOK.

P8 – [100%] Welke informatie (inzicht) heeft u nodig van deelnemers om voor de aanbesteding van de raamovereenkomst een passende inschrijving te kunnen doen? Houdt er rekening mee dat er binnen de raamovereenkomst nog minicompetities uitgevoerd moeten worden om de concrete opdrachten te kunnen verstrekken. In deze minicompetities kan/moet meer gedetailleerde achtergrondinformatie verstrekt worden.

Hoe concreter en vollediger de scope en randvoorwaarden worden beschreven, hoe beter leveranciers hun aanbod/capaciteit en prijs kunnen afstemmen. Idem voor het verwachte aantal opdrachten per tijdsperiode of jaar (evt. verdeeld over type pentests en deelnemers, abonnementsvormen), type systemen (web, infra, API, Cloud, mobiel, OT), omvang (bijv. aantal IP's), verwachte doorlooptijd en specifieke doelstellingen of compliance-eisen (bijv. BIO, NIS2, bepaalde standaarden). Aanvullend is ook relevant: veiligheids(screenings)- of VGB-eisen, mate van onsite-werk (op locatie), voorbeeldcasussen, duidelijk omschreven deliverables en randvoorwaarden (eisen aan rapportages, toe te passen standaarden, personeel).

P9 – [100%] Welke ervaring heeft uw organisatie met vrijwaringsverklaringen die nodig zijn bij de start van een pentest, maar door betrokkenen niet tijdig genoeg ondertekend worden en de start van een pentest ophouden? Welke aandachtspunten en/of tips kunt u meegeven?

Veel respondenten herkennen dat vrijwaringsverklaringen vaak vertraging bij opdrachtgevers veroorzaken door late juridische afstemming of onduidelijkheid over tekenbevoegdheid. Bij testen in systemen van derden kan dat bijzonder lastig zijn. Enkelen achten het dan ook reëel dat kosten van vertraging door opdrachtgever mogen worden doorbelast. Veel kan worden voorkomen met standaardisatie (standaardverklaring op ROK-niveau) en duidelijke afspraken vooraf over verantwoordelijkheidsverdeling (eventueel richting een doorlopende vrijwaringsverklaring op ROK-niveau met automatische werking of aanvulling op NOK-niveau) en eenduidige escalatielijnen. Daarnaast het bewustzijn creëren bij opdrachtgevers om bij een eventuele derde partij tijdig aandacht te vragen voor de vrijwaringsverklaringen (minimaal 2-4 weken voor start/intake pentest initiëren). Liefst wordt de opdracht ingepland na het doorlopen van het vrijwaringsproces en ontvangst van de vrijwaring.

P10 – [95%]Zijn er pentesters/dienstverleners die al rekening houden met AI en Quantum cryptografie componenten bij pentesten? Hoe zou u deze elementen in een marktbenadering (aanbesteding) zinvol ingebed zien?

De meeste partijen houden rekening met AI (phishing, exploitatie) en quantum (cryptografie), al ziet men dit nu nog niet als standaard c.q. dagelijkse praktijk, maar wel relevant als optioneel (risicoanalyses en advisering) toekomstgericht thema, zowel als onderdeel van de testmethodologie als testobject. Het advies is het opnemen als differentiator of optioneel specialisme in de aanbesteding (minicompetities) of

innovatietrajecten, zodat de ROK toekomstgericht blijft zonder drempels onnodig te verhogen. Als concrete suggesties wordt gegeven: cryptoregistratie als voorbereiding op post-quantum cryptografie en integratie van AI-kwetsbaarheden in rapportages.

P11 – [100%] Is het vereiste van een CCV-keurmerk of gelijkwaardig nuttig als geschiktheidseis (knock out)? Zo ja waarom, zo nee waarom niet?

Men is verdeeld over het gebruik van CCV-keurmerk Pentesten. Het keurmerk of een vergelijkbare accreditatie kan dienen als kwaliteitsfilter, maar ook onnodig (grotere, internationale) partijen mogelijk uitsluiten en kostenverhogend werken.
Circa 16% van de respondenten vindt het CCV-keurmerk nuttig (kwaliteit waarborg, uniform kader) en benoemen geen nadelen.
Circa 42% van de respondenten raadt het eisen van een CCV-keurmerk (of gelijkwaardig) af: ze vinden het te beperkend en geen nuttig vereiste, het sluit (onnodig) goede en grotere, internationale partijen uit. De kwaliteit van pentesten zit vooral in mensen/methodiek en rapportagekwaliteit; minder in een keurmerk dat dan een schijnzekerheid geeft over de kwaliteit. Ook zijn vereisten van CCV-keurmerk soms conflicterend met klantvereisten (met name rond geheimhouding) en/of ze vinden het keurmerk onnodig kostenverhogend. Zij pleiten vooral voor het stellen van inhoudelijke eisen en wensen, zonder keurmerk of accreditatie.
De overige 42% aan respondenten benoemen zowel voor- als nadelen van het CCV-keurmerkvereiste. Men waarschuwt voor te strikte toepassing van het CCV-keurmerkvereiste en benadrukken het nut/ de noodzaak om ruimte te houden voor alternatieven ('CCV of gelijkwaardig'), met soms alternatieve certificeringen als voorbeelden (CREST, ISO 17025, ISO 9001/27001 + specifieke aanvullingen voor pentesten, OSCP, CHECK (Brits), ANSSI (Frans) of ENS (Spaans)) of anders (indien de lat lager gelegd wordt) het keurmerk als zwaarwegend subgunningscriterium te gebruiken.

P12 – [90%] Welke subgunningscriteria kunnen naar uw beeld het beste worden ingezet in de keuze van opdrachtnemers voor de raamovereenkomst? En welke subgunningscriteria stelt u dan voor mededinging (minicompetities) bij de verstrekking van nadere overeenkomsten voor?

In de ROK (raamovereenkomst) is het zinvol de nadruk te leggen op kwaliteit methodiek (PTES, OWASP) en afstemming hierover, ervaring/referenties, aantoonbare expertise en (toekomstgerichte) ontwikkeling/borging van expertise, security maturity en beveiligingsmaatregelen, certificering, continuïteit en flexibiliteit/schaalbaarheid en soms innovatie (AI, automatisering). In de NOK (nadere overeenkomsten) kan de nadruk liggen op een concreet plan van aanpak, beschikbaarheid en doorlooptijd, passende expertise in team, prijs/prestatie en aansluiting op specifieke scope, risico's en context. Ook specifieke toegevoegde waarde (tooling, rapportage, ondersteuning), afstemming op volwassenheid opdrachtgever en innovatie is genoemd. Men geeft ook mee de prijs beperkt te wegen ten opzichte van de kwaliteit. Er worden suggesties gedaan voor proeven van bekwaamheid (praktijktest), casusopdrachten en voorbeeldrapportages. Ook toepassing van meer interactieve vormen zijn genoemd (discussies, uitwisseling van ideeën, workshops, bevindingen meeting etc.). Een paar respondenten adviseren in het geheel geen minicompetities te houden, maar bijvoorbeeld een roulatiesysteem toe te passen.

P13 – [100%] In bijlage 2 bij dit document treft u een conceptversie van het programma van eisen aan. Bij de totstandkoming van deze versie van het programma van eisen is gebruik

gemaakt van de Methodiek voor Informatiebeveiligingsonderzoek met Audit Waarde (MIAUW), waarin suggesties voor inkoopeisen voor pentesten zijn opgenomen, maar zijn ook aanvullingen en aanpassingen op MIAUW gemaakt om beter tegemoet te komen aan de diversiteit van behoeftes van betrokken Deelnemers. Wat vindt u van de voorliggende conceptversie van het programma van eisen? Bij uw beantwoording gaat u bij voorkeur in op de volgende subvragen: a. Welke eisen moeten naar uw mening vervallen of afgezwakt worden om te voorkomen dat u en/of andere potentiële inschrijvers hier niet aan kunnen/willen voldoen (verlagen instapniveau)? Motiveer uw antwoord. b. Welke eisen moeten naar uw mening nog toegevoegd of strikter gesteld worden om risico's voor Deelnemers te beperken/minimaliseren (verhogen instapniveau)? Motiveer uw antwoord. c. Welke andere suggesties wilt u doorgeven?
Het concept Programma van Eisen (PvE) is een goede basis, maar veel respondenten vinden het zwaar in detail en met veel administratieve (rapportage)eisen. Dit wordt regelmatig als nadeel van MIAUW genoemd. Respondenten vragen om verlichting van overbodige of verouderde eisen, versterking van kwaliteit en opvolging, en een pragmatische, proportionele aanpak die bruikbaarheid vooropstelt. Te verlagen of schrappen eisen: • De verplichting om zeer uitgebreide detailplannen (zoals testcases of alle technische stappen) vooraf op te leveren is soms disproportioneel, zeker bij kleine opdrachten of spoedtrajecten. Dit leidt tot bureaucratie, vertraging en beperkt de flexibiliteit die vaak juist nodig is bij pentesten. Ook is suggestie gedaan meer ruimte te zoeken om de vergaande afstemming voor start pentest te verplaatsen na aanvaarding scope (plan van aanpak). Probeer administratieve lasten te beperken, o.a. door bondiger plan van aanpak. • Sommige eisen schrijven dwingend voor dat rapportages exact een bepaalde indeling moeten volgen, wat de creatieve en inhoudelijke vrijheid van testers beperkt. Leveranciers willen hun rapportage kunnen afstemmen op specifieke klantbehoeften. • De handtekening rapporteur zou volgens enkele respondenten niet nodig zijn, de rapportage is bedrijfsverantwoordelijkheid. Een ander vindt de versiebeheertabel een voldoende vervanging van de handtekening. Een respondent vindt het belangrijk om geen namen van de overige personen die betrokken zijn bij het onderzoek te benoemen in een rapport dat openbaar kan komen, om hen hiermee te beschermen. Handtekening van externe peer reviewer is m.n. bij gerubriceerde informatie problematisch. • Standaarden en methodieken: Maak duidelijk maken dat er ruimte is voor gelijkwaardige methodieken naast de reeds genoemde, eventueel onderbouwd, maar schrijf de methodieken niet normatief en limitatief voor. Een respondent waarschuwt voor het stapelen van allerlei normenkaders en adviseert een leidende te kiezen. • Certificeringen personen: geef meer ruimte en sta gelijkwaardige alternatieven toe, inclusief aantoonbaar gelijkwaardige ervaring. Overweeg verwijzing naar (standaard) de laatste versie van het kwalificatieschema van CCV (keurmerk pentesten). Certificeringsvereisten van de eindverantwoordelijke rapporteur(s) loslaten, maar aan de uitvoerende testers koppelen. Sommige vinden het goed dat bewijsmiddelen gevraagd worden, een enkele vindt dat dit niet per opdracht maar centraal geregeld moet worden. • Sta voor technische inhoud ook Engels toe (niet alleen NL). • Assume breach past slecht bij blackbox pentesten. Zet deze selectief in bij grey- en whitebox.

- Eisen die nog SHA-1 hashes of classificaties voorschrijven worden als verouderd beschouwd en voegen weinig waarde toe. SHA-2/3 of moderne hash-methoden zijn de huidige standaard. Overweeg selectievere toepassing, b.v. alleen waar onweerlegbaarheid van informatie essentieel is voor de uitkomsten.
- De CIA-classificatie per bevinding is vaak te gedetailleerd, tijdrovend en niet altijd relevant; opdrachtnemers geven de voorkeur aan flexibeler risicoclassificatie (bijv. CVSS). Naast CVSS-score ook kans x impact? Overzicht door opdrachtgever aangeleverde CIA-scores in managementsamenvatting lijkt wat te theoretisch.
- Verplichte bijlagen/bestanden: De (ruwe) scanoutput wordt vaak gezien als overbodig en belastend. Het voegt vaak geen meerwaarde toe voor de opdrachtgever en leidt tot dikke rapporten met beperkte bruikbaarheid. Beschrijving alle ontvangen bestanden en documenten (inclusief hashes) ook daarom alleen op verzoek opdrachtgever. Een respondent vindt de checklist per standaard onnodig kostenverhogend.
- Tijdlijn: niet altijd nodig, overweeg alleen kritieke acties, alleen testperiode of volledig weg te laten. Minder gebruikelijk. Maakt evt. detailniveau van tijdslijn helder.
- Bewijslast: niet altijd mogelijk, kijk naar inspanningsverplichting.
- Een Root-cause-analyse is niet altijd zinvol en reëel (bij te weinig diepgang en context).
- Documenteren toegangswegen: geen aanpassing testobject, scope en data, is b.v. alleen al door wijziging logbestand of sessietoken niet mogelijk, ook alle (soms duizenden) kwetsbaarheden uit automatische test handmatig verifiëren is te strikt.
  Verplichte vulnerability disclosure via NCSC verruimen, om uitsluiting van internationaal erkende disclosure processen te voorkomen. Sluit aan bij CVE-standaard.
- Delen rapport met derden kan niet zonder afspraak met opdrachtnemer.
- Verwerkersovereenkomst alleen opstellen/voorschrijven als die juridisch noodzakelijk is.
- Intake hoeft niet per se binnen 5 werkdagen. Geef meer ruimte. Maak ook duidelijker wanneer de termijn start.

Strikter te stellen eisen of toe te voegen eisen:

1. Een pentest levert pas waarde als bevindingen ook leiden tot verbeteringen. Daarom moet opvolging en advisering nadrukkelijk onderdeel zijn van de opdracht, bijvoorbeeld verplichte hertesten of validatie van mitigaties.
   Opdrachtnemers kunnen (optioneel) ook adviseren met leerrapporten of thema's met onderliggende oorzaken.
2. Enkele respondenten vinden dat eisen moeten worden aangescherpt om nieuwe dreigingsvormen (AI-gegenereerde aanvallen, deepfakes, geautomatiseerde exploit generatie) te kunnen adresseren.
3. Voor een deugdelijke risico-inschatting is het zaak toelichting verlangen bij elke bevinding.
4. Vraag om meer transparantie van opdrachtnemers over te gebruiken tools
5. Stel strengere eisen aan de vaardigheden van testers (bijvoorbeeld OSCP, OSEP of vergelijkbare certificaten) om kwaliteit en betrouwbaarheid te waarborgen.
   Een respondent adviseert duidelijkere eisen te stellen aan het door opdrachtnemers verder mogen uitbesteden (aan onderaannemers), om het risico op onvoldoende kwaliteitstoezicht te beperken.
6. Scope-onderdeel: OT als afzonderlijk toepassingsgebied opnemen.
7. De eisen voor veiligheidsscreening (VGB) en omgang met gerubriceerde informatie moeten duidelijker en uniformer worden vastgelegd, zodat leveranciers vooraf weten waaraan ze moeten voldoen. Opdrachtgever zou veiligheidsscreening moeten faciliteren en betalen.
   Een respondent adviseert om screening en vrijwaring op ROK-niveau vast te leggen.
   Overweeg voor gevoelige omgevingen specifiekere afspraken over gegevensverwerking

(o.a. versleuteling, bewaartermijn en bewijs van veilige verwijdering) en om opslag en verwerking van hoger gerubriceerde gegevens vanuit opdrachtgever te faciliteren. Let ook op toepassing Nederlandse jurisdictie in plaats van die van het land van de fysieke locatie van de test.

Overige suggesties:

- Eisen moeten uitvoerbaar en kostenefficiënt zijn, en niet leiden tot onnodige administratieve lasten. Kleine opdrachten moeten eenvoudiger kunnen worden ingericht.
- De nadruk moet liggen op duidelijke, praktisch toepasbare rapportages met bruikbare resultaten en aanbevelingen in plaats van juridisch-formele eisen die weinig toevoegen. Overweeg hiernaast een eis van kwaliteitscontrole voor oplevering rapportage.
- Voor opdrachten die staatsgeheime informatie raken, moet de opdrachtgever de speciale infrastructuur en juridische borging faciliteren. Leveranciers beschikken daar meestal niet over.
- Leveranciers zien graag een gemeenschappelijk kader, maar met de mogelijkheid om aan te sluiten bij specifieke klantbehoeften en sectorspecifieke eisen (bijvoorbeeld in zorg of financiële sector). Een respondent vindt vooral gemeenschappelijke consistentie van belang (geen afwijkingen tussen opdrachtnemers toestaan), waarbij wellicht na een pilot-fase bekeken kan worden welke rapportage-eisen aanpassing behoeven.
  Verduidelijk terminologie, m.n. rol intake en start test.
- Stimuleer samenwerking tussen lokale en wereldwijde expertise.
- Specificeer een indicatief tijdbudget per testtype. Dit ondersteunt uniform beoordelen en voorkomt te lage biedingen met weinig diepgang.

P14 – [100%] Als bijlage 2 bij dit document treft u een conceptversie van het programma van eisen aan. Bij dit programma van eisen is een modelrapportage gevoegd. Deze modelrapportage kent een standaard opzet/indeling, gebaseerd op de diverse eisen. Bij toekomstige verstrekking van een opdracht (pentest) wordt verwacht dat een opdrachtnemer op basis van de uitgevoerde pentest een rapportage oplevert, conform de vastgestelde modelrapportage, met standaard hoofd- en paragraafindeling. Dit model moet zorgen voor uniformiteit, transparantie, compleetheid van de rapportage en reproduceerbaarheid van het onderzoek.
Opdrachtgever kan nieuwe versies van dit model vaststellen, die opdrachtnemer daarna dient toe te passen. Opdrachtnemer heeft tijdens de looptijd van de raamovereenkomst de mogelijkheid suggesties aan opdrachtgever te geven voor verbetering van het model. Afwijking van dit model is alleen toegestaan na schriftelijke goedkeuring van Deelnemer, overeen te komen in het plan van aanpak (pre-engagement) van een pentest.

a. Wat vindt u van de opzet (indeling) van de huidige versie van de modelrapportage?
b. Welke wijzigingen moeten naar uw mening in de modelrapportage doorgevoerd worden (toevoegingen, wijzigingen, verwijderingen)?

Een modelrapportage wordt nuttig geacht voor uniformiteit, vergelijkbaarheid, auditwaarde en transparantie, reproduceerbaarheid, bruikbaarheid voor technische en niet-technische stakeholders. Opdrachtgevers kunnen dan ook eenvoudiger benchmarken en trends analyseren. Een eenduidige structuur helpt ook toezichthouders en audits. Er is niettemin een minderheid die voorstelt geen modelrapportage te gebruiken en eventueel alleen de te adresseren onderwerpen in de rapportage voor te schrijven.
Belangrijkste verbeterpunten:

- Toevoegen: duidelijke managementsamenvatting met kernbevindingen en risicogroepering, sectie met strategische aanbevelingen, een trendanalyse (bijvoorbeeld herhaalde kwetsbaarheden of structurele problemen), mogelijk ook met sectie over

detectie- en responscapaciteit (hoe goed is een organisatie erin geslaagd aanvallen te signaleren of te stoppen).
- Aanpassen: meer flexibiliteit om rapportages op klantsituatie af te stemmen, niet een verplicht format hanteren. Na sluiten raamovereenkomst met opdrachtnemers een gedragen rapportageformat bepalen. Aparte sectie opnemen voor verantwoording over hulpmiddelen en detectiemethodiek, expliciete verwijzing naar gebruikte standaarden/methodieken per fase.
- Verwijderen/verlichten: Reacties komen overeen met die op de vorige vraag (P13). Verplichte (ruwe) scanoutput, te gedetailleerde bijlagen, leiden tot overmatig lange rapportages. Dit leidt soms tot onnodig dikke rapporten (hogere kosten), details worden vaak niet gelezen, zorg dat de informatie beter aansluit bij de doelgroep. Meer optioneel. Beheer van testresultaten, w.o. afspraken over versleutelde opslag en bewaartermijnen, niet in rapportage. Idem voor checklists per standaard en beschrijving van hulpmiddelen, inclusief URL's. Namen en certificeringen van uitvoerende testers ter bescherming van hun privacy niet verplicht opnemen. Tijdslijn met uitgevoerde acties optioneel. Apart hoofdstuk conclusies kan evt. vervallen, want generieke conclusies over de veiligheid kunnen vaak niet getrokken worden op basis van een pentest, bovendien kunnen aanbevelingen in samenvatting.
- Taalgebruik: rapportage in Engels toestaan met Nederlandse samenvatting, om internationale partijen niet uit te sluiten.

Een modelrapportage is overwegend gewenst en nuttig, mits flexibel, beknopter en bruikbaarder gemaakt voor verschillende doelgroepen. Kernbevindingen en bruikbare aanbevelingen moeten centraal staan, terwijl overbodige of te gedetailleerde onderdelen optioneel/facultatief moeten worden.

P15 – [50%] Hieronder is ruimte voor uw eventuele aanvullende reactie.

Enkele partijen voegen extra aandachtspunten toe die buiten eerdere vragen vallen:
- Integratie met bredere securityprocessen: koppeling met (security) monitoring (NDR), assetmanagement/CMDB en centrale security dashboards.
- Her-testen/remediatie validatie: standaardoptie voor borging mitigatie (sluiten kwetsbaarheden).
- Veilige overdracht van testresultaten: via documentbeheersystemen.

Sommige partijen herhalen eerdere punten, w.o. de gewenste splitsing pentesten/red teaming; PTES bruikbaar mits flexibel; afraden van minicompetities; beperken van bewijs- en rapportagelast (nadeel MIAUW).
Verdere aanvullingen gaan vooral over borging, opvolging en integratie in bredere security.

3.2 Red Teaming

In totaal hebben 18 partijen op het deel Red teaming gereageerd, waarvan 11 vaak uitgebreid antwoord of toelichting geven.

R1 – [100%] Hoe kunnen we inspelen op verwachting rond in te zetten capaciteit in de uitvoering en dat wat als verwachting door de leverancier is opgegeven voor de ROK, gegeven de schaarste aan ART/TIBER ervaring in de markt en de grote vraag bij organisaties (met name financiële instellingen vanuit DORA-regelgeving)?

Een meerderheid onderschrijft de schaarste in beschikbare capaciteit in de markt voor Red Teaming, mede door DORA/TLPT . Coördinatie van (voorgenomen/in het vooruitzicht gestelde) Red Teaming tests binnen de overheid in combinatie met een (binnen grenzen) concrete planning (o.a. ruim vooraf) kunnen helpen de opdrachten in de markt te absorberen. Ook wordt in overweging gegeven om de schaarste te beperken door toegangsdrempels iets te verlagen.
R2 – [100%] Wat is uw beeld bij het aantal Red Teaming-partijen bij een raamovereenkomst? Relevante elementen zijn onder andere hoeveel ART/TIBER testen u zou kunnen uitvoeren, naast wat u nu al doet (dus: wat u beschikbaar zou hebben voor deze ROK), dan wel het maximaal aantal deelnemers dat u (gelijktijdig) kunt bedienen. Het is essentieel dat we een beeld hebben van het absorptievermogen in de markt is en hoe daarop evenwichtig kan worden ingespeeld.
Een aantal van circa 6 partijen wordt genoemd. Grotere aantallen lijken de voorkeur te zijn van mogelijk nieuwe toetreders. Ook nu wordt het belang van planning benoemd.
R3 – [95%] Heeft u suggesties op welke wijze de beoogde aanbesteding voor een raamovereenkomst naar uw inzicht kan bijdragen aan het vergroten van het speelveld van marktpartijen die ervaring hebben met het ART/TIBER, voor partijen die dat bij inschrijving op de aanbesteding niet hebben? Wat zijn dan de essentiële kwaliteitsaspecten van een inschrijver zonder ART/TIBER ervaring, die bij eventuele gunning van de raamovereenkomst wel opdrachten van deelnemers voor Red Teaming testen conform ART of TIBER op kwalitatief beoogde wijze moeten kunnen uitvoeren?
Er is draagvlak voor het meenemen van Red Teaming-ervaring anders dan TIBER/ART in de gunningcriteria. Daarnaast is het advies te werken met een groeimodel.
R4 – [100%] In bijlage 3 bij dit document treft u een conceptversie van het programma van eisen aan op basis van ART/TIBER. Wat vindt u van de voorliggende conceptversie van het programma van eisen? Bij uw beantwoording gaat u bij voorkeur in op de volgende subvragen: a. Welke eisen moeten naar uw mening vervallen of afgezwakt worden om te voorkomen dat u en/of andere potentiële inschrijvers hier niet aan kunnen/willen voldoen (verlagen instapniveau)? Motiveer uw antwoord. b. Welke eisen moeten naar uw mening nog toegevoegd of strikter gesteld worden om risico's voor Deelnemers te beperken/minimaliseren (verhogen instapniveau)? Motiveer uw antwoord. Welke andere suggesties wilt u doorgeven?
Hier wordt gepleit voor een aantal versoepelingen, zoals de NL taal-eis, rapportage, VOG/VGB, te gebruiken templates et cetera.
R5 – [90%] Welke subgunningscriteria dragen volgens u het beste bij aan de keuze van een ROK-partner en welke voor de NOK?
Genoemde voorstellen voor subgunningscriteria richten zich op de individuele expertise, de (gezamenlijke) kwaliteit van teams en relevante ervaring.

R6 – [90%] Welke subgunningscriteria dragen volgens u het beste bij aan de keuze voor een Threat Intelligence Provider?
Diverse suggesties gedaan die nogal uiteenlopen. Deze zijn waardevol om nader te bekijken voor de rol van de Threat Intelligence-provider als deze onderdeel uitmaakt van een Red Teaming-opdracht.
R7 – [65%] Hieronder is ruimte voor uw eventuele aanvullende reactie.
Een divers beeld, waarbij partijen soms voorstellen de (toetredings-)drempels van de TIBER-standaard te verlagen. Verder wordt afstemming met andere sectoren (e.g. de financiële sector) benoemd om capaciteit in de markt over Red teaming opdrachten te verdelen.

3.3 SOC-diensten

S1 – [95%] Is de duiding van type M&D/KS&R-diensten herkenbaar en sluit deze aan op door u te leveren producten? Zijn er ontbrekende diensten?
De huidige duiding van M&D en KS&R diensten wordt breed herkend en vormt een solide basis. Tegelijkertijd adviseren meerdere marktpartijen om actuele ontwikkelingen en moderne SOC-functionaliteiten explicieter in de scope mee te nemen. Dit draagt bij aan toekomstbestendige, geïntegreerde en effectieve dienstverlening. De modulaire opbouw wordt overwegend als positief ervaren — marktpartijen herkennen en waarderen de opzet van de markconsultatie die uitgaat van een 'startpakket' en 'aanvullende diensten'. Er is nog wel behoefte aan verduidelijking rond het startpakket versus aanvullende diensten, vooral m.b.t. SIEM en logmanagement. Een aantal partijen vraagt brede aandacht voor aanvullende beveiligingslagen (e-mail, identiteit, web, remote access), wat de traditionele M&D/KS&R scope verbreedt. ➢ Veel partijen herkennen de basisdiensten terug in hun portfolio, zoals 24/7 monitoring, incident response, vulnerability management, threat intelligence, en integratie met diverse IT-omgevingen (on-prem, cloud, endpoints). ➢ De beschrijvingen van M&D en KS&R sluiten aan bij moderne SOC-aanpakken, vaak gebaseerd op frameworks als NIST-CSF. ➢ Diverse aanbieders bieden modulaire en schaalbare diensten aan, afgestemd op klantbehoefte en maturity. ➢ Er is herkenning van onderscheid tussen detectie/rapportage (MSSP) en beheer/mitigatie (MSP), wat cruciaal is voor duidelijke rolverdeling. ➢ Verschil en samenhang tussen startpakket en aanvullende diensten: meerdere marktpartijen vragen verduidelijking over het onderscheid tussen bijvoorbeeld SIEM in het startpakket versus Security Log Management als aanvullende dienst. ➢ Incident Response en Threat Intelligence worden soms als zelfstandige IB-diensten geplaatst. Men hecht eraan het belang van integratie van deze componenten in SOC-diensten te benadrukken. Breed geadviseerde aanvullende of meer actuele dienstcomponenten: • *Continue risicobeoordeling en integratie van CTI* (Cyber Threat Intelligence) - Monitoring van dreigingsinformatie en het vertalen daarvan naar detectie- en responsacties (Continuous Threat Exposure Management, CTEM).

- *Exposure Management en Attack Surface Management* (ASM/CAASM) - Proactief inzicht en beheer van de aanvalsvlakken (exposure) en kwetsbare assets.
- *Automatisering van respons* (SOAR) - Geautomatiseerde responsprocessen en playbook-gedreven workflows binnen afgesproken service windows.
- *Beheer en optimalisatie van SOC- en SIEM-platformen* - Engineering, tuning en doorontwikkeling van detectieregels en platformen als aparte dienstcomponenten.
- *Threat Hunting en Behavioral Analytics* - Proactieve detectie van onbekende of geavanceerde dreigingen door analyse van gedrag en anomalieën.
- *Bescherming en monitoring van aanvullende aanvalsvectoren* - Specifiek genoemd: e-mailbeveiliging en monitoring, identiteitsmonitoring (o.a. lekken van credentials), webverkeer en remote access monitoring. Ook OT/IoT-monitoring wordt door enkele partijen als belangrijk en toekomstgericht genoemd.
- *Breach and Attack Simulation* (BAS) - Tools en diensten voor het continu testen van effectiviteit van controls en detectiemaatregelen.

Specifieke aanvullingen:
- Onderscheid tussen detectietechnieken (NDR, EDR, SIEM) en let ook op technieken die nu lijken te ontbreken, zoals honeypots en applicatiebewaking.
- Belang van SIEM-integratie en extra diensten zoals malware-analyse en gebruikersgedreven threat reporting.

S2 – [95%] Kunt u dienstverlening bieden volgens de opzet van M&D-diensten met daarin een Startpakket en aanvullende diensten en ziet u dit ook als handzame opzet voor organisaties om snel met een SOC te kunnen beginnen met mogelijkheden tot groei? Dit ook ten aanzien van het eenmalig in minicompetitie komen in de context van een raamovereenkomst.

De overgrote meerderheid van de respondenten geeft aan dienstverlening te kunnen bieden conform de voorgestelde opzet van een startpakket met aanvullende diensten. Deze modulaire werkwijze wordt breed herkend als werkbaar en praktisch, met name in combinatie met een raamovereenkomst waarin via een eenmalige minicompetitie gunning plaatsvindt. De modulaire opzet goed aansluit bij de marktvraag: organisaties kunnen snel starten met basisfunctionaliteit, laagdrempelig instappen (variërend van instapniveau tot high-end SOC-functionaliteit, inclusief use case-uitbreiding, CTEM, SOAR, etc.), en de dienstverlening vervolgens gefaseerd uitbreiden/groeien. Het biedt voorts flexibiliteit en aanpasbaarheid aan klantspecifieke infrastructuur, maturity en dreigingsbeeld. Deze aanpak sluit goed aan op bij diverse partijen bestaande onboarding- en groeimodellen, wat implementatie vereenvoudigt. Verschillende marktpartijen hebben het startpakket al geïntegreerd in hun bestaande SOC-dienstverlening, inclusief onderdelen als SIEM, CTI, basale use cases en identity monitoring. De voorgestelde structuur van een startpakket met uitbreidbare modules wordt breed gezien als werkbaar, schaalbaar en toekomstgericht, mits:
- het startpakket functioneel voldoende dekking biedt en toekomstbestendig is;
- de afbakening tussen startpakket en aanvullende diensten helder en eenduidig is (o.a. overlap tussen startpakket en aanvullende diensten, zoals SIEM en Security Log Management, wat voor verwarring kan zorgen);
- de inrichting van de minicompetitie zorgvuldig gebeurt, zodat prijsduiking en ongewenste risicoverplaatsing worden voorkomen.

Waarschuwing I: een te beperkt startpakket kan leiden tot suboptimale keuzes:
1. Puntoplossingen die later lastig integreerbaar zijn,

2. Onvoldoende beveiligingsniveau bij aanvang,
3. Verlies van efficiëntie en toekomstbestendigheid.
4. Één van deze partijen pleit ervoor om elementen zoals logmanagement en Network Detection & Response (NDR) altijd in het startpakket op te nemen, ook als dat betekent dat minder partijen kunnen inschrijven.

Waarschuwing II: eenmalige minicompetitie kan het risico brengen dat aanbieders onrealistisch lage prijzen voor het startpakket aanbieden in de hoop winst te maken op de later af te nemen aanvullende diensten, met mogelijk daaruit voortvloeiende onderdekking en een onhoudbaar businessmodel. Ook wordt opgemerkt dat het effectiever is om direct een volwassen dienst te leveren i.p.v. gefaseerd.

S3 – [95%] Wat zijn de meest belangrijke KPI's waarmee de prestaties van M&D en KS&R dienstverlening zijn te meten en aan te tonen?

Er is brede consensus over belang van het meten van prestaties met goed gedefinieerde KPI's voor zowel Monitoring & Detectie (M&D) als Kwetsbaarheid Scanning & Rapportage (KS&R). De genoemde KPI's zijn in vier hoofdgroepen onder te brengen:

1. <u>Operationeel (voornamelijk M&D)</u> **-** snelheid, nauwkeurigheid en beschikbaarheid van detectie- en responsprocessen:
   a) Mean Time to Detect/Respond – eerste detectie van een incident/start van opvolging of mitigatie;
   b) Time to Escalate/Act – nadere onderverdelingen van reactietijden.
   c) False/True Positive Rate – kwaliteit van detectie en efficiëntie van triage.
   d) Beschikbaarheid SOC / SIEM tooling – uptime van monitoringsystemen.
   e) Aantal incidenten, meldingen of alerts per maand (inclusief afhandelingsstatus).
   f) SLA-naleving per incidenttype en prioriteit - tijdigheid van dienstverlening.

   De KPI onder a) & b) worden breed gezien als dé centrale KPI's voor M&D. Ook asset coverage is bij vrijwel iedereen een kernindicator.

2) <u>KS&R-specifiek</u> - volledigheid, relevantie en opvolging:
   a) Aantal en ernst van gedetecteerde kwetsbaarheden - *vaak gerelateerd aan CVSS-scores.*
   b) Time-to-remediation / herstelsnelheid - *tijd tot mitigatie of oplossing.*
   c) Slaagpercentage van scanning runs - *technische kwaliteit van de scanuitvoering.*
   d) Scanfrequentie & dekking van assets - *volledigheid van de scope.*
   e) Aantal retained kwetsbaarheden of terugkerende issues - *effectiviteit van opvolging.*
   f) Er is een relatieve onderbelichting van KS&R in sommige antwoorden.

   De uitwerking van deze KPI's is minder concreet en soms beperkt tot scanfrequentie en rapportagetijd. Ook lopen benaderingen meer uiteen: van 'KPI's bij KS&R minder geschikt' tot 'veel KPI's gebruiken' (zoals dekking, risicoscores, herstelsnelheid).

3) <u>Kwaliteits- en effectiviteit</u> - Deze KPI's meten hoe goed de dienstverlening daadwerkelijk bijdraagt aan veiligheid:
   a) Coverage van MITRE ATT&CK (TTP's en detectieregels) – inzicht in scope en diepgang van detectie.
   b) Effectiviteit van detectieregels (bijvoorbeeld via Use Case testing).
   c) Threat hunting resultaten / sightings op CTI feeds – actieve dreigingsopsporing.

d) Outcome-driven metrics / Return on Security Investment (ROSI) – meetbare risicoreductie.
e) Aantal herhaalincidenten en opvolging RCA-aanbevelingen.

4) Governance, rapportage en klantgerichtheid - transparantie en samenwerking:
a) Tijdigheid en volledigheid van rapportages (maandelijks, realtime dashboards).
b) Klanttevredenheid (CSAT scores).
c) SLA-compliance over dienstverleningselementen heen.
d) Effectiviteit van kennisoverdracht bij hybride modellen.
e) Aantal en impact van beveiligingsvergaderingen (feedbackloops).

Aanvullend:
- Business Use Cases het uitgangspunt vormen bij het inrichten van SOC-dienstverlening. KPI's worden dan daarop afgestemd.
- Meerdere respondenten benadrukken dat KPI's afgestemd moeten zijn op de volwassenheid van de klant, het dreigingsbeeld, de impact op kritieke bedrijfsprocessen (business-driven security) en op risico's die de bedrijfscontinuïteit, reputatie of compliance direct raken.
- Visualisatie via dashboards en integraties (bijv. XSOAR, ServiceNow, Sentinel) om KPI's toegankelijk te maken voor verschillende doelgroepen binnen de klantorganisatie.
- Gebruik van het MITRE ATT&CK-framework als referentie voor detectiecapaciteit.
- Threat hunting en zicht op actuele dreigingen (bijvoorbeeld statelijke actoren) worden in toenemende mate als kwaliteitsmaatstaf ingezet.

S4 – [100%] Kunt u zich met betrekking tot de gevraagde M&D en KS&R dienstverlening onderscheiden van andere marktpartijen. Zo ja, op welke punten onderscheidt u zich en hoe zijn deze punten meetbaar of aantoonbaar?

1) Schaalbaarheid en operationele capaciteit
- 24/7 monitoring via internationale SOC's met "follow-the-sun"-modellen
- Volledig Nederlands SOC of EU-georiënteerde levering, inclusief lokale taal en compliance
- Snelle onboarding en deployment, in sommige gevallen binnen 2 weken

Meetbaar via: aantal SOC's, aantal analisten, onboardingtijd, beschikbaarheid, SLA's.

2) Geavanceerde technologie en integraties
- Eigen security-platformen (proprietary SIEM, XDR of SOAR), inclusief agentic AI en automatisering
- Gedragsgebaseerde detectie (UEBA) i.p.v. IOC's
- Externe platformintegraties (bijv. Tenable, Qualys, Fortinet, Exabeam, Microsoft Defender).

Meetbaar via: aantal logbronnen, MTTR/MTTD, false positive ratio's, integratieoverzichten.

3) Kwaliteit van detectie en dreigingsinformatie
- Eigen dreigingsinformatie via grote telemetrie-netwerken of red teams
- Sectorspecifieke use cases (bijv. Rijksoverheid, onderwijs, zorg) en mapping op MITRE ATT&CK
- Threat-led of contextuele detectie op basis van organisatie- of persona-profielen

Meetbaar via: use case-bibliotheken, MITRE-mapping, incidenten per sector, KPI-rapportages.

4) Security governance en dienstverlening op maat
   - Security-as-a-service governance modellen met SDM/TAM, strategische reviews, escalatieprocessen.
   - Inzage in performance en radicale transparantie richting klanten.
   - Modulair opgebouwde dienstverlening met groeipad en schaalbare architectuur.

   Meetbaar via: SLA's, klanttevredenheid, governance-documentatie, aantal maatwerkanalyses.

5) Compliance, certificeringen en wet- en regelgeving
   - ISO 27001, SOC 2, NIST, BIO, PCI-DSS, TIBER-EU.
   - Lokale dataopslag en EU-soevereiniteit, inclusief bescherming tegen de US Cloud Act.

   Aantoonbaar via: certificaten, auditlogs, compliance-routes, referentiecases.

6) Kwetsbaarhedenscanning (KS&R)
   - Continue of gestructureerde scanning, gekoppeld aan risicobeoordeling.
   - Integratie met scanplatformen zoals Qualys, Tenable, SonarQube.
   - Rapportage gericht op risico en mitigatieadvies.

   Meetbaar via: aantal kwetsbaarheden per scan, mitigatiepercentage, rapportkwaliteit.

7) AI, automatisering en innovatie
   - Gebruik van AI en ML voor triage, weak signal detection en automatisering.
   - SOAR-playbooks en geautomatiseerde respons zijn veelgenoemd, vaak met meetbare MTTR-resultaten.

   Meetbaar via: aantal playbooks, MTTR/MTTD, aantal geautomatiseerde incidenten.

Ook in dit kader genoemd: onafhankelijkheid van Big Tech; snelle MTTR's met concrete benchmarks; integrale securityvisie en samenwerking binnen het ecosysteem.

S5 – [95%] Met betrekking tot het aanvraagproces en het aansluiten van ICT-assets:
- Hoe snel en eenvoudig is het aanvragen en aansluiten van het Startpakket voor M&D-diensten?
- Welk type informatie heeft u daarvoor nodig van een deelnemer?
- Welke inspanningen moet een deelnemer zelf uitvoeren?
- Wat zijn overige randvoorwaarden?

Snelheid en eenvoud:
Connectiviteit is een sterk bepalende factor voor de doorlooptijd. Één partij geeft aan vaak in één dag aan te kunnen sluiten, mits een standaardconfiguratie. Anderen stellen binnen 2 weken te operationaliseren voor zover het een standaardomgeving (startpakket & Microsoftproducten) betreft. De meeste respondenten bewegen tussen 2 tot 12 weken, afhankelijk van complexiteit. Bij veel maatwerk kan het tot 6 maanden kan duren. Factoren die invloed hebben op snelheid: beschikbaarheid van Microsoft E5/Sentinel | volwassenheid IT-omgeving (standaardisatie vs. maatwerk) | bestaande logging / infrastructuur | interne capaciteit bij deelnemer (technisch personeel, projectleiding).

Benodigde informatie om M&D-dienstverlening te operationaliseren:

Inventaris van ICT-assets (servers, werkstations, netwerk, OT/IoT) | Netwerkdiagrammen/ -schema's | Logbronnen (firewalls, AD, endpoints, cloud, etc.) | Kroonjuwelen/kritieke processen | Securitybeleid, risk profile, use cases | Authenticatie gegevens/accounts/AD/ licenties | contactpersonen en escalatieprocessen.

Inspanningen deelnemer:
Aanleveren van technische informatie/documentatie | Configureren van logbronnen | Installeren van agents / sensoren | Meewerken aan sessies/intake/use cases | Faciliteren van toegang/credentials/VPN | Aanpassen van firewallregels/netwerk | Contact-/aanspreekpunt | Monitoring van logvolumes.

Overige randvoorwaarden:
Bereikbaarheid systemen / netwerktoegang | Standaardprotocollen of tooling (Syslog, API, MS-stack) | Microsoft-licenties en Azure tenant (min. E3, bijv. E5 voor Sentinel)| Governance en samenwerking |Technische compatibiliteit/security policies | Beschikbaarheid testomgeving / infrastructuur | Deelname aan business use case-sesssie | Juridische borging (NDA, dataverwerking, vrijwaring) | Monitoring/rapportage/audit-ondersteuning.

Overige bevindingen:
- Microsoft-gebaseerde omgevingen (E5, Sentinel) maken snelle aansluiting makkelijker.
- Breed draagvlak voor een gefaseerde onboarding-aanpak, vaak startend met kritieke logbronnen en use cases.
- Standaardproces met ruimte voor maatwerk.
- Relatie tussen implementatiesnelheid en kwaliteit van de detectiedienst (bijvoorbeeld minder false positives bij zorgvuldige onboarding).

S6 – [95%] Wat is naar uw inzicht een reëel te verwachten en voor u acceptabele periode van af-/aansluiten waarop een deelnemer kan beslissen tot afname, dan wel van een opdrachtnemer afscheid te nemen? Welke randvoorwaarden zijn hier aan de orde?

Aan- en afsluitperiode: circa 4 tot 12 weken. Gemiddeld is 5 tot 8 weken een werkbare termijn. Dit omvat de technische implementatie, organisatorische besluitvorming en het operationeel gereed te maken van de dienstverlening, inclusief technische configuratie, inrichting van rapportages en het afstemmen van prioriteiten. De periode is afhankelijk van de complexiteit van de omgeving en de benodigde voorbereidingen en mate van onboarding. Na het aansluiten volgt een opstartperiode van circa 6 maanden om de dienstverlening te implementeren en optimaliseren. Hierna zijn meer flexibele, maandelijkse contracten mogelijk. Voor het beëindigen van de samenwerking wordt doorgaans een opzegtermijn van 1 tot 3 maanden gehanteerd. Deze termijn biedt voldoende ruimte voor een zorgvuldige overgang, waarbij afspraken over dataoverdracht, continuïteit van monitoring en kennisdeling worden gewaarborgd. Ook hier: een optimale duur hangt af van contractuele voorwaarden en de complexiteit van de overdracht.

Randvoorwaarden:
- Beschikbaarheid van benodigde informatie en contactpersonen bij de deelnemer
- Realistische planning afgestemd op capaciteit van beide partijen
- Duidelijke afspraken over overdracht van data, logbestanden en configuraties
- Exit-strategie en zorgvuldige transitie, inclusief knowledge transfer
- Waarborging van continuïteit van monitoring tijdens transitie

- Compliance met wettelijke en contractuele vereisten
- Flexibiliteit om hybride modellen en veranderende omstandigheden te accommoderen
- Eigenaarschap van data blijft bij de deelnemer, inclusief volledige export en verwijdering na beëindiging
- De periode voor een soepele overgang en afronding ligt vaak tussen 4 weken en 3 maanden, waarbij er nadruk ligt op een warme overdracht en het voorkomen van serviceonderbrekingen.

Overige bevindingen:
- Koppeling implementatietijd aan het aantal FTE van de te monitoren organisatie (vuistregel: 1 week per 1.000 FTE).
- Langere opstartperiode (tot 6 maanden) voor het goed landen van de dienst versus kortere technische implementatietermijnen (1-2 weken tot 8 weken) afhankelijk van de complexiteit van de omgeving.
- Minimale contractduur van 3 jaar.
- Heldere afspraken over overdracht van data en configuraties, inclusief het eigenaarschap en het verwijderen van data na beëindiging.
- Mate van flexibiliteit en de mogelijkheid tot maandelijkse opzegbaarheid na een initiële periode (wenselijk, maar niet altijd standaard aangeboden).
- Belang van samenwerking en actieve betrokkenheid voor change management en beschikbaarheid van technische resources.
- Duidelijke exit-strategie, inclusief het vastleggen van afspraken over verantwoordelijkheden en compliance, om risico's bij beëindiging te beperken.

S7 – [95%] In geval van opvolging van een voorgaande SOC-dienstverlener: maakt dit uw antwoord op S6 anders? Zo ja, hoe?

De meeste marktpartijen geven aan dat een opvolging van een voorgaande SOC-dienstverlener niet per se leidt tot een fundamentele wijziging in de aanpak of de looptijd van het onboardingproces. Wel zijn er nuances in hoe deze overgang wordt ingevuld:

- *Nieuwe implementatie*: overstap is een nieuwe implementatie, waarbij altijd een eigen analyse, inrichting en onboarding plaatsvindt, in nauwe afstemming en een formeel overdrachtsmoment met de vertrekkende partij om continuïteit te waarborgen.
- *Fase-in periode*: 1 tot 3 maanden voor kennisoverdracht, SIEM-tuning, validatie van use cases, data migratie en hertraining van SOC-analisten. Dit is belangrijk voor het waarborgen van kwaliteit en het vermijden van hiaten in monitoring.
- *Versnelde onboarding door bestaande infrastructuur*: mogelijke versnelling als een deel van de infrastructuur en processen al aanwezig is. De mogelijkheid om bestaande logbronnen en use cases te importeren kan de overgang verkorten. Tegelijkertijd is er tijd nodig voor een grondige kennisoverdracht en integratie om risico's te beperken.
- *Ongewijzigde looptijd, gewijzigde handelingen*: in de eerste weken ligt de focus op het veilig uitfaseren van de oude dienst en het gefaseerd opbouwen van de nieuwe SOC-dienst met basis visibiliteit en afgestemde rapportages.
- *Complexiteit en langere doorlooptijd bij transities*: opvolging leidt vaak tot langere onboarding periodes door complexiteit in data-migratie, systeemcompatibiliteit, regelmapping en kennisoverdracht. Dit kan de doorlooptijd verlengen van standaard 2-4 weken naar 4-6 weken en in complexe legacy-omgevingen zelfs tot 8-16 weken. Ook: extra kosten en de noodzaak van parallelle operationele periodes om monitoring-gaps te voorkomen.

- *Essentie van duidelijke afspraken en samenwerking*: goede afstemming met de vertrekkende SOC, heldere afspraken over data-export, en een zorgvuldig overdrachtsproces cruciaal zijn om continuïteit, kwaliteit en beheersbare kosten te garanderen.

S8 – [95%] Welke (minimale) looptijd van nadere overeenkomsten adviseert u? U kunt hierbij desgewenst onderscheid maken tussen de verschillende diensten die afgenomen kunnen worden binnen de raamovereenkomst. Houd rekening met verschillende implementatietijden, terugverdientijden, exit-/retransitietijden etc.

- Minimale looptijd van 24 tot 36 maanden voor kern SOC/MDR-diensten.
- Looptijden korter dan 2 jaar worden over het algemeen als onvoldoende gezien om zowel technische als organisatorische optimalisaties en een stabiele dienstverlening te waarborgen.
- Voor specifieke, aanvullende diensten of modules zoals Threat Intelligence (TI), Forensics, Vulnerability Management (VOC), of ad-hoc opdrachten wordt vaak een kortere looptijd (12 tot 24 maanden) genoemd, mits deze losstaan van de kern-MDR-dienst.

Diensttype	**Advies minimale looptijd**	**Motivatie / toelichting**
Monitoring & Detectie (M&D)	24–36 maanden	Implementatie, tuning, contextvalidatie, opbouw van detectiecapaciteit, volwassenwording SOC. Sommige partijen adviseren zelfs 3-5 jaar (Marktpartij-8, 14).
Kennisdeling, Signalering & Respons (KS&R)	12–24 maanden	Afhankelijk van intensiteit en integratie met deelnemer; lagere initiële kosten en kortere terugverdientijd.
Vulnerability Onderzoek/-Beheer (VOC)	Minimaal 2 jaar, bij voorkeur 3 jaar	Meerdere scan-fixcycli nodig, trendanalyse, contextopbouw.
Specifieke modules (TI, Forensics, …)	12-24 maanden	Lagere implementatie-investering, kortere terugverdientijd.

Motivatie langere looptijd (24–36 maanden of langer):

- *Implementatie en afstemming*: onboarding, tuning van detectieregels, integratie met processen en tooling, kennisoverdracht.
- *Terugverdientijd*: investeringen in tooling, procesinrichting en kennisopbouw moeten zich kunnen terugbetalen.
- *Stabiliteit en volwassenheid*: tijd nodig om SOC-dienst te laten groeien van basisoperatie naar volwassen, geoptimaliseerde service.
- *Exit en retransitie*: voldoende ruimte voor soepele overgang en dataoverdracht bij beëindiging (meestal 1–3 maanden).
- *Kostenbeheersing*: langere contracten spreiden initiële investeringen en zorgen voor lagere jaarlijkse kosten.
- *Continuïteit* en innovatie: langere looptijden stimuleren continue verbetering, innovatie en schaalvoordelen.

Overige bevindingen:

- Initiële looptijd van 36 maanden met verlengingsopties.
- Langere looptijden tot 4-5 jaar of zelfs 8 jaar om strategische samenwerking en optimale benutting van investeringen mogelijk te maken.
- Bij tijdelijke of kleinere opdrachten kunnen kortere looptijden van 12 tot 24 maanden passend zijn, maar vaak tegen hogere kosten.
- Bij hybride of complexe omgevingen een langere initiële looptijd vanwege extra afstemming en risico's.
- Vooraf contractueel vast te leggen van verlengingsmogelijkheden en exit-regelingen ten behoeve van de flexibiliteit en continuïteit.

S9 – [100%] Zijn er mogelijkheden – en zo ja welke – om naast de eerstelijns ondersteuning van opdrachtgever en eventuele specialisten ook één of enkele medewerkers van deelnemer in deze rollen te laten meewerken en zo een hybride situatie in te richten?

Vrijwel alle marktpartijen ondersteunen een hybride situatie of staan daar positief tegenover, mits er duidelijke afspraken zijn over rollen, toegang, mandaten en communicatie. Hybride samenwerking wordt gezien als bevorderlijk voor kennisdeling, eigenaarschap, betere afstemming op de organisatiecontext en continuïteit. De vormen van de beschreven hybride situaties lopen uiteen van een volledige integratie in operationele SOC-taken tot strategische advisering en de rol van business context provider door de deelnemer. De optimale vorm van hybride samenwerking hangt af van de gewenste betrokkenheid van de deelnemer, de volwassenheid van de interne organisatie, en het serviceniveau van de SOC-dienstverlener. Voor structurele samenwerking is aandacht nodig voor juridische, organisatorische en operationele aspecten (zoals SLA's, compliance en datatoegang).

Vorm	**Omschrijving**
Volledige integratie in SOC-operatie	Deelnemers draaien mee in eerstelijns- of specialistische rollen (bijv. triage, analyse, engineering).
Strategische samenwerking / advisering	Deelnemers leveren context, prioriteren assets, valideren workflows, geven input op detectie-use cases.
Security liaison	Medewerker van deelnemer fungeert als brug tussen organisatie en SOC voor contextverrijking, impactanalyse en interne coördinatie.
Toegang tot tooling en dashboards	Deelnemer krijgt inzicht in meldingen, dashboards en kan (beperkt) meewerken aan analyses.
Training en kennisoverdracht	Marktpartijen bieden trainingen aan, on-site of online, en stimuleren meedraaien voor kennisopbouw.

<u>Technische en organisatorische voorwaarden:</u>

- Heldere afspraken cruciaal: RACI-modellen, SOP's, Document Afspraken en Processen (DAP), mandaten.
- Beveiligde toegang tot tooling vereist, inclusief RBAC voor rolverdeling en toegangsbeheer.
- Samenwerkingsmodellen worden vaak afgestemd tijdens onboarding.
- Continu overleg en afstemming zijn nodig om hybride modellen effectief te houden.

<u>Aandachtpunten:</u>

- *Duidelijkheid over verantwoordelijkheden:* Veel partijen benadrukken het belang van duidelijke taakverdeling om conflicten te vermijden bij incident response, SLA's en KPI's. Eigenaarschap over incidenten moet ondubbelzinnig geregeld zijn.
- *Beperkingen bij 24/7 inzet:* Enkele partijen geven aan dat structurele inzet van personeel van deelnemer voor 24/7-dienstverlening lastig is, i.v.m. capaciteitsplanning, compliance en toegang tot klantdata van andere deelnemers.
- *Capaciteit en locatie-afhankelijkheid:* Geografische beperkingen (bijv. max. 1 uur reistijd) kan fysieke samenwerking beïnvloeden.
- *Risico's van operationele verwarring:* Één partij waarschuwt voor hybride modellen waarin incident eigenaarschap en SLA-beheersing kunnen vervagen. Men adviseert om de operationele verantwoordelijkheid volledig bij het SOC te laten en de deelnemer een adviserende rol te geven.

Best Practices:

- Deelname aan een Cyber Intelligence Extension Program als voorbeeld van een succesvol embedded/hybride model.
- Gebruik van co-working platforms met gezamenlijke incidentafhandeling (inclusief taaktoewijzing en notities) als faciliterende technologie.

S10 – [95%] Gelden bovenstaande antwoorden voor het Startpakket ook voor de aanvullende M&D-diensten of spelen daar andere aandachtpunten of verschillen?

Consensus: de eerder gegeven antwoorden zowel van toepassing zijn op het Startpakket, als de aanvullende diensten. Tegelijkertijd: aanvullende diensten brengen vaak extra complexiteit, technische eisen, governance-afspraken en afhankelijkheden met zich mee:

- Uitgebreidere voorbereiding en integratie nodig
- Langere implementatietermijnen door complexiteit en afhankelijkheden
- Aanvullende eisen aan beveiliging, compliance of operationele processen
- Meer aandacht voor Goverance en RACI nodig in hybride situaties
- Schaalbaarheid
- Rol van de deelnemer [wordt groter]
- Kosten-batenverhouding
- Meer afstemming en extra tooling
- Exit-complexiteit neemt toe [door aanvullende diensten]

Opvallende reactie: implementatietijden bij aanvullende diensten zijn korter, omdat ze voortbouwen op de bestaande infrastructuur van het Startpakket.

S11 – [95%] Zijn er mogelijkheden of beperkingen of bijzonderheden met betrekking tot het monitoren van Clouddiensten waar in het kader van SOC-diensten rekening mee moet worden gehouden? Zo ja, welke?

Mogelijkheden:

- *Cloud-native integraties:* Veel marktpartijen bieden standaardkoppelingen met grote cloudplatformen zoals Microsoft Azure, Microsoft 365, AWS, Google Cloud en SaaS-applicaties. Native connectors en API's zorgen voor real-time toegang tot logs, alerts en gedragsdata.
- *API-gedreven monitoring:* Door gebruik te maken van API's kunnen security-gegevens uit clouddiensten in SIEM-, SOAR- of XDR-platforms worden geïntegreerd, waarmee automatische detectie en response mogelijk is.

- *Gebruik van gespecialiseerde cloudbeveiligingstools:* CSPM (Cloud Security Posture Management), CWPP (Cloud Workload Protection Platforms) en cloud-native securitytools zoals Microsoft Defender for Cloud, Crowdstrike en Prisma worden breed ingezet.
- *Integratie in bestaande SOC- en SIEM-omgevingen:* Cloudlogs worden gekoppeld aan on-premises data, waardoor volledige correlatie en inzicht ontstaat.
- *Flexibiliteit in tooling:* Marktpartijen stemmen tooling af op de wensen en architectuur van de deelnemer en bieden vaak maatwerkoplossingen.
- *Security-processen en -beheer:* Naast technische monitoring zijn er duidelijke afspraken over verantwoordelijkheden, zoals het beheren van toegangsrechten, het opvolgen van alerts en het uitvoeren van remediërende acties door de deelnemer.

Beperkingen en aandachtpunten:

- *Toegangsrechten en tenantbeheer:* Voor het ontsluiten van logs zijn expliciete rechten nodig (bijvoorbeeld audit- of reader-rollen), wat in multi-tenant- en hybride omgevingen complex kan zijn.
- *Licentie- en configuratiebeperkingen:* De beschikbaarheid en kwaliteit van logging zijn afhankelijk van het licentiemodel en configuratie (bijv. Microsoft E3 vs. E5), wat invloed heeft op detectiemogelijkheden.
- *Datacompliancy en privacy:* Cloudmonitoring moet voldoen aan privacywetgeving zoals de AVG/GDPR en NIS2, inclusief afspraken over dataopslag, retentie en filtering van persoonsgegevens.
- *Complexiteit door multi-cloud en hybride omgevingen:* Het monitoren van meerdere cloudproviders kan extra integratiecomplexiteit en langere implementatietijden met zich meebrengen.
- *Scope en verantwoordelijkheden:* Monitoring omvat niet alleen infrastructuurlogs, maar ook applicatie- en API-logs. De deelnemer is vaak verantwoordelijk voor installatie van agents en opvolging van incidenten.
- *Beperkingen in geavanceerde analyses:* Basale cloudmonitoringdiensten bieden doorgaans geen diepgaande forensische of malware-analyses; die zijn vaak aanvullend of handmatig.
- *Integratie met ticketing en workflow:* Er wordt ondersteuning geboden voor integratie met ticketsystemen, vaak in één- of tweerichtingsverkeer, ter optimalisatie van incidentafhandeling.

Aanbevelingen:

- Cloudmonitoring vanaf het begin (‘by design’) van Cloudomgevingen meenemen.
- Tijdens onboarding moeten Cloud-omgevingen, licenties, toegangsrechten en monitoringvereisten duidelijk vastleggen.
- ‘Least privilege’-principes toepassen voor toegangsrechten om risico’s te minimaliseren en toch volledige zichtbaarheid te waarborgen.
- Aandacht voor het onderhouden en configureren van Cloud-native securitytools, en voor het periodiek valideren van detectielogica en responsprocessen.
- Heldere afspraken over datatoegang, scheiding en compliance bij multi-tenant en hybride omgevingen.

S12 – [95%] Zijn er mogelijkheden/aandachtspunten met betrekking tot een koppeling met het ticketsystem van een opdrachtgever?

De meeste respondenten bieden API- en webhook-functionaliteiten aan, waarmee integraties kunnen worden gerealiseerd met gangbare ITSM-platformen zoals ServiceNow, TOPdesk, Jira, en in sommige gevallen ook andere systemen (mits deze beschikken over goed

gedocumenteerde API's). De koppelingen kunnen zowel uni- als bi-directioneel zijn, afhankelijk van de wensen en processen van de opdrachtgever. De integratie stelt organisaties in staat om incidenten, meldingen, en statusupdates automatisch bij te houden en te synchroniseren tussen systemen, zodat zowel de SOC-leverancier als de opdrachtgever altijd toegang hebben tot dezelfde actuele informatie.
Daarnaast wordt vaak een flexibele aanpak geadviseerd, waarbij de integratie zorgvuldig wordt afgestemd op de specifieke eisen en processen van de deelnemer. De implementatie van de koppeling gebeurt vaak in een gezamenlijke fase met de deelnemer, waarbij technische afstemming, zoals de configuratie van ticketvelden en prioriteiten, wordt besproken. Een testfase voorafgaand aan de livegang is in de meeste gevallen aanbevolen om de werking te waarborgen.

Aandachtpunten:

- *Toegangsbeheer en autorisatie:* Voor een veilige en betrouwbare koppeling is het essentieel dat alleen bevoegde gebruikers toegang hebben tot de systemen en dat de juiste autorisaties zijn ingesteld.
- *Beveiliging van gegevens:* Het waarborgen van de bescherming van uitgewisselde gegevens is cruciaal, bijvoorbeeld door gebruik te maken van encryptie en veilige opslagmethoden. Dit is van belang om te voldoen aan privacywetgeving en compliance-eisen.
- *Procesafstemming:* Er is vaak een duidelijke noodzaak om het procesmodel van de opdrachtgever af te stemmen met het SOC, bijvoorbeeld wie verantwoordelijk is voor triage, opvolging en afmelding van incidenten. Het is belangrijk dat de samenwerking en verantwoordelijkheden duidelijk zijn, vooral bij complexere organisatiestructuren.
- *Data minimalisatie en compliance:* Er moet aandacht worden besteed aan het overdragen van alleen noodzakelijke gegevens, in lijn met privacywetgeving en interne compliance-eisen.
- *SLA-afstemming en ticketstructuur:* Het is belangrijk om vooraf duidelijke afspraken te maken over de SLA's, ticketstructuur, statusvelden en eigenaarschap van incidenten. In sommige gevallen blijft het SOC-systeem leidend, in andere gevallen is het ticket van de opdrachtgever leidend.
- *Mogelijke complexiteit bij meerdere betrokken partijen:* Wanneer meerdere afdelingen of organisaties betrokken zijn, kan de integratie van verschillende ticketsystemen technische en procesmatige dilemma's met zich meebrengen. Dit kan leiden tot complexiteit, maar met een goed integratieplan zijn deze problemen doorgaans oplosbaar.

Aanbevelingen:

- In een vroege fase van de implementatie een gedetailleerde technische en functionele afstemming te doen, en een testplan op te stellen om de integratie in een gecontroleerde omgeving te testen voordat deze live gaat.
- Stel de samenwerking en afstemming tussen de technische teams van de opdrachtgever en de SOC-leverancier centraal om een soepele en flexibele integratie te waarborgen.
- In gevallen waar er wijzigingen zijn in het ticketsysteem of andere systemen van de opdrachtgever (bijvoorbeeld updates aan firewalls of andere infrastructuur), kan het nodig zijn om de integratie opnieuw te evalueren en bij te stellen.

S13 – [95%] Welke mogelijkheden biedt u als opdrachtnemer om deelnemers via een uniform dashboard/interface visueel inzicht te geven in loginformatie en events? Het is van belang dat deelnemers alleen de eigen informatie zien en geen inzicht krijgen in informatie van andere deelnemers.

De meeste marktpartijen bieden uniforme dashboards die deelnemers real-time visueel inzicht geven in de log- en eventinformatie die specifiek voor hen relevant is. Deze dashboards zijn vaak interactief en aanpasbaar, zodat deelnemers de weergave kunnen afstemmen op hun eigen voorkeuren en behoeften (bijvoorbeeld met widgets of filters). De dashboards geven inzicht in belangrijke informatie zoals beveiligingsincidenten, trends, KPI's, en de status van incidenten en alerts.
In de meeste gevallen wordt een multi-tenant architectuur gebruikt, wat betekent dat elke deelnemer zijn eigen geïsoleerde omgeving krijgt binnen het platform. Dit zorgt ervoor dat gegevens van andere deelnemers niet toegankelijk zijn. De rol-gebaseerde toegangscontrole (RBAC) wordt vaak toegepast om ervoor te zorgen dat deelnemers alleen toegang hebben tot de gegevens die relevant zijn voor hen. Deze toegangscontrole is meestal fijnmazig ingesteld, zodat verschillende gebruikers binnen een deelnemende organisatie toegang hebben tot alleen de voor hun rol relevante informatie.
Daarnaast bieden sommige marktpartijen exportmogelijkheden voor loggegevens naar een externe SIEM-omgeving, zoals Syslog, LEEF, of CEF-formaat, zodat deelnemers hun gegevens verder kunnen analyseren of integreren met hun bestaande systemen. Dit maakt het mogelijk om een naadloze integratie te realiseren voor deelnemers die al gebruik maken van een eigen SIEM-systeem.

Aandachtspunten:

- *Data-isolatie:* garantie volledige datascheiding tussen deelnemers. Dit wordt technisch geborgd door het gebruik van tenant- of homegroup-isolatie en role-based access control (RBAC). Elke deelnemer heeft alleen toegang tot zijn eigen data en geen inzage in die van andere deelnemers, wat cruciaal is voor privacy en compliance.
- *Customisatie van dashboards:* dashboards afstemmen op de specifieke behoeften van de deelnemer, bijvoorbeeld op basis van sector-specifieke eisen (zorg, onderwijs, overheid) of interne KPI's. Sommige partijen adviseren om in de onboardingfase samen met de deelnemer de belangrijkste stuurinformatie vast te stellen, zodat de dashboards optimaal aansluiten bij de behoeften van de CISO of operationele teams.
- *Flexibiliteit en uitbreidingsmogelijkheden:* o.a. het toevoegen van maatwerkrapportages of de mogelijkheid om logdata te exporteren naar andere systemen. Dit zorgt ervoor dat het dashboard niet alleen functioneel is voor het huidige gebruik, maar ook kan meegroeien met de behoeften van de deelnemer in de toekomst.
- *Security:* Strikte toegangscontrole met o.a. multi-factor authenticatie (MFA) en opties om audit logs bij te houden voor compliance en beveiliging.

Aanbevelingen:

- In de onboardingfase is het nuttig om duidelijk te definiëren welke gegevens en visualisaties voor de deelnemer relevant zijn, zodat het dashboard vanaf het begin goed aansluit bij de informatiebehoefte van de gebruiker.
- Periodieke reviews van de dashboards kunnen helpen om deze te blijven afstemmen op veranderende behoeften of nieuwe dreigingsscenario's.
- Samenwerking met de deelnemer voor het integreren van bestaande systemen zoals SIEM-tools of rapportageplatforms kan de effectiviteit van de oplossing vergroten, vooral bij organisaties die al beschikken over een goed ingerichte IT- en beveiligingsinfrastructuur.

S14 – [95%] Zijn er mogelijkheden dat medewerkers van deelnemende diensten ook toegang krijgen tot monitoringsystemen (b.v. SIEM) van opdrachtnemer om zo zelf zaken in te zien en queries te doen? Zo ja, beschrijf op hoofdlijnen welke functionaliteiten toegankelijk zijn.

Algemene trends:

- Read-only toegang is de standaardoptie voor medewerkers van deelnemende diensten, zodat ze geen wijzigingen kunnen aanbrengen in het monitoringsysteem.
- Beveiligde dashboards of eigen SIEM-omgevingen per deelnemer om data en analyses toegankelijk te maken zonder dat er toegang is tot de data van andere deelnemers.
- Rol-gebaseerde toegang (RBAC) en datascheiding zijn een veelvoorkomende maatregel om privacy en integriteit te waarborgen.
- De toegang tot queries, rapportages en alerts wordt vaak aangeboden, maar zonder wijzigingsrechten in de configuratie van het SIEM-systeem.
- Volledige toegang tot SIEM-omgevingen wordt soms geboden als de deelnemer zelf het beheer van het SIEM heeft, bijvoorbeeld via Microsoft Sentinel.

Onderstaand in de tabel een weergave van resondenten en de geboden functies.

	Marktpartij												
Functies	2	4	6	7	8	9	10	12	13	14	16	20	21	22
Dashboard	✓				✓	✓	✓	✓		✓			✓	✓
Read-only toegang (queries)	✓	✓	✓		✓					✓	✓	✓		✓
Query's uitvoeren	✓	✓	✓	✓	✓	✓	✓		✓	✓			✓	✓
Alerts bekijken	✓	✓	✓	✓	✓	✓	✓		✓	✓			✓	✓
Alerts classificeren/taggen	✓			✓		✓	✓							✓
Rapportages genereren	✓	✓	✓		✓	✓	✓		✓	✓		✓	✓	✓
Exports van data	✓													
Zelf detecties maken				✓			✓							
Zelf incidenten analyseren		✓	✓	✓	✓	✓	✓		✓	✓			✓	✓
Maatwerk queries uitvoeren					✓	✓	✓			✓			✓	✓
Incidentbeheer via XSOAR										✓				
Datascheiding en privacy waarborgen	✓			✓	✓		✓	✓		✓			✓	✓
Multi-Factor Authenticatie (MFA)					✓								✓	✓

Datascheiding en privacy waarborgen en Multi-Factor Authenticatie (MFA) zijn strikt genomen geen functionaliteit on informatie in te zien, maar worden als randvoorwaarden genoemd.

Enkele respondenten gaat uit van de aanwezigheid van een SIEM bij Opdrachtgever. Meestal gaat men dan uit van Microsoft Sentinel en maakt op deze wijze gebruik van SIEM-

functionaliteit van Opdrachtgever/deelnemer. Het beheer en de toegang tot het Sentinel-SIEM ligt in dat geval volledig bij Opdrachtgever/Deelnemer.

S15 – [95%] Een aantal deelnemende diensten beschikken reeds over Microsoft E5 licenties. Welk effect van deelnemers met Microsoft E5-licenties ziet u op uw dienstverlening, zowel qua verantwoordelijkheden als in de prijsstelling?

De meerderheid van de respondenten ziet de aanwezigheid van Microsoft E5-licenties als een positieve factor die de integratie vergemakkelijkt en de efficiëntie van de dienstverlening verhoogt. In het bijzonder doordat E5 toegang biedt tot Microsoft Defender, Microsoft Sentinel en gerelateerde securitycomponenten. Velen geven aan dat zij hun dienstverlening zodanig hebben ingericht dat deze naadloos integreert met de E5-stack, en dat zij kunnen aansluiten op reeds aanwezige tooling in de omgeving van de deelnemer. Een minderheid werkt met eigen endpoint agents die parallel aan of in plaats van Microsoft Defender worden ingezet. In die gevallen wordt Defender vaak in "passive mode" gebruikt. Deze partijen benadrukken voordelen op het gebied van digitale autonomie en onafhankelijkheid van niet-Europese technologieën.

Verantwoordelijkheidsverdeling:
- De deelnemer is verantwoordelijk voor het beheer en de activatie van de E5-licenties en de bijbehorende configuratie van Microsoft-tools.
- De dienstverlener draagt zorg voor detectie, analyse, alertverwerking, rapportage en/of aanvullende taken zoals ruleset tuning, incident response en threat intelligence-integratie.

Effect op prijsstelling:
De aanwezigheid van E5-licenties leidt tot een verlaging van kosten voor tooling, met name doordat licentiekosten voor Microsoft Defender en Sentinel al zijn afgedekt. Hierdoor worden alleen operationele SOC-diensten (zoals monitoring, detectie en incident response) nog in rekening gebracht. Veel leveranciers hanteren een BYOL-model (Bring Your Own License) en maken een onderscheid tussen:
- Microsoft-verbruikskosten (zoals log ingestie en retentie), die voor rekening van de deelnemer komen en;
- SOC-dienstverlening, die separaat wordt geprijsd.

M.b.t. de aanbesteding: er wordt gewezen op de noodzaak van een transparant prijsmodel, waarin Microsoft-gerelateerde kosten (zoals ingestiekosten in Sentinel) expliciet moeten worden meegenomen, eventueel op basis van fictieve logvolumes. Dit maakt onderlinge vergelijking van inschrijvingen eerlijker en voorkomt verborgen kosten.

Overige bevindingen:
- Duidelijke verantwoordelijkheidsafbakening is cruciaal. Er moet expliciet worden afgesproken wie wat configureert, wie welke toegang heeft, en wie verantwoordelijk is voor monitoring, respons en compliance.
- Diversiteit in integratiestrategieën: Sommige partijen integreren direct met Microsoft Sentinel, anderen voeren de gegevens in eigen SIEM-omgevingen in of gebruiken aanvullende tooling (zoals eigen agents).
- Impact op kostenstructuur verschilt per leverancier. Een aantal partijen wijst op het risico dat traditionele SOC-modellen niet goed vergelijkbaar zijn met E5-gebaseerde modellen zonder duidelijke volumetrische aannames.

- EU-soevereiniteit: Een kleine groep leveranciers positioneert zichzelf nadrukkelijk als alternatief voor Amerikaanse technologie (zoals Microsoft) in lijn met strategische overwegingen van de Rijksoverheid.
- Licentieactivatie en datatoegang: niet alle E5-componenten zijn standaard actief. Dit vereist verificatie tijdens onboarding. Ook toegang tot gegevens, rechten in portals en API's moeten afgestemd worden.

S16 – [95%] Het ligt in de lijn der verwachting dat de kwaliteit van de dienstverlening toeneemt naarmate een marktpartij gedurende langere tijd diensten levert aan een deelnemer, doordat er ervaring wordt opgebouwd.
Onderschrijft u dit beeld? Op welke onderdelen is deze kwaliteitsverbetering volgens u zichtbaar en meetbaar?

Het is consensus dat de kwaliteit van de dienstverlening verbetert naarmate de samenwerking met een deelnemer langer duurt door toenemende kennis van de IT-omgeving, processen, risico's, prioriteiten en organisatiecultuur van die deelnemer. De kwaliteitsverbetering manifesteert zich in:

1. Detectie en analyse
- Use cases worden steeds beter afgestemd op de specifieke infrastructuur, dreigingsscenario's en risicoacceptatie van de deelnemer.
- Door contextualisatie en fine-tuning neemt het aantal false positives af en worden incidentmeldingen relevanter en nauwkeuriger.
- Er ontstaat een grotere true positive rate en een verbeterde signaal-ruisverhouding in detecties.

2. Incidentrespons en operationele samenwerking
- SOC-analisten en klantteams raken beter op elkaar afgestemd, wat leidt tot kortere responstijden (MTTR) en snellere detectie (MTTD).
- Playbooks worden specifieker en effectiever doordat zij worden aangepast aan de feitelijke processen en verantwoordelijkheden van de deelnemer.
- Incidenten worden sneller en adequater opgevolgd dankzij betere communicatie en bekendheid met escalatieprocedures.

3. Rapportage en sturing
- Rapportages en dashboards sluiten steeds beter aan bij de informatiebehoeften van de deelnemer.
- KPI's verschuiven van generiek naar klantspecifiek, en worden inzichtelijker en waardevoller.
- Periodieke evaluaties zorgen voor structurele verbetering van de dienstverlening (bijv. via SLO-gesprekken, tactische reviews of strategische sessies).

4. Strategische meerwaarde en innovatie
- Langdurige samenwerking leidt tot gezamenlijke ontwikkeling van een security roadmap, integratie met GRC-processen en hogere security maturity.
- De opgebouwde relatie bevordert proactief handelen, innovatie en het snel implementeren van nieuwe technologieën en threat intelligence.
- In sommige modellen (zoals groeimodellen of maturity frameworks) groeien operationele, tactische en strategische samenwerking met de deelnemer mee over tijd.

5. Meetbaarheid van kwaliteitsverbetering
- KPI's zoals MTTD, MTTR, alertvolume, true/false positive ratio
- Klanttevredenheidsonderzoeken en feedbackloops
- MITRE ATT&CK-dekking

- Periodieke maturity assessments
- Kwalitatieve input uit evaluatiegesprekken en reviews

Overige bevindingen:

- *Kwaliteitsgroei is initieel het grootst:* Diverse marktpartijen geven aan dat in de eerste maanden van samenwerking de meeste winst wordt behaald, bijvoorbeeld in het reduceren van false positives en het verbeteren van incidentafhandeling.
- *Samenwerking en vertrouwen zijn sleutelbegrippen:* Kwaliteit neemt niet alleen toe door technische tuning, maar ook door het opbouwen van persoonlijk vertrouwen en nauwe samenwerking tussen klant en SOC.
- *Contextkennis maakt het verschil:* Diepere kennis van businesskritische assets, netwerkstructuren en interne processen leidt tot een relevantere, effectievere SOC-dienstverlening.
- *Security wordt een gezamenlijke verantwoordelijkheid:* Leveranciers positioneren zichzelf als partner in een 'cyberbeveiligingsteam', waarin zij samen met de klant de beveiliging continu verbeteren.
- *Strategische betrokkenheid neemt toe over tijd:* Een aantal leveranciers zet in op samenwerking op strategisch niveau (boardroom-briefings, threat landscape updates), wat de impact en toegevoegde waarde vergroot.
- *Niet meetellen van inwerkperiode in contractduur:* Indien de contractduur wordt gebruikt voor prestatievergelijking of verlenging, is het raadzaam om rekening te houden met een aanlooptijd waarin de dienstverlening nog niet op piekniveau is.

S17 – [95%] Bij inschrijving op de aanbesteding zullen prijscomponenten opgenomen worden die bepalend zijn op het niveau van de raamovereenkomst (ROK). Deze zullen gelden voor alle nadere offertes (en daarmee nadere overeenkomsten/NOKs) van deze inschrijver binnen de raamovereenkomst. Op basis van welke eenheden per dienst kan een beheersbare prijs worden bepaald? Het gaat om prijscomponenten waaruit een prijs wordt opgebouwd en wat de 'drivers' zijn die de prijs kunnen of zullen doen stijgen of dalen. Het doel is te komen tot en veralgemeniseerd prijsmodel waarin diverse inschrijvers kunnen worden vergeleken.

Algemene structuur van prijsmodellen (vaak modulair opgebouwd) bestaat uit de volgende componenten:

- Eenmalige kosten (onboarding/implementatie)
- Terugkerende vaste kosten (per maand/jaar)
- Variabele kosten (op basis van gebruik/schaal/complexiteit)

Dienst	Basiseenheden prijs	Veelvoorkomende 'drivers' voor stijging/daling
Monitoring & Detectie (M&D)	✓ Aantal logbronnen / logsources ✓ Aantal assets (endpoints, servers, firewalls) ✓ Volume logdata (GB/dag of Events per Second (EPS)) ✓ Aantal gebruikersaccounts ✓ Type technologie (SIEM, EDR, NDR) ✓ Detectiecomplexiteit / aantal use cases	✓ Toename logbronnen ✓ Complexiteit van IT/OT-omgeving ✓ Volume data ✓ Licentiewijzigingen bij leveranciers ✓ Mate van geautomatiseerde respons (SOAR)
Incident Response / Forensics	✓ Uren (strippenkaarten / bundels) ✓ Aantal incidenten of responsetijd	✓ Aantal of zwaarte van incidenten ✓ SLA-niveau (24/7 of kantoortijden)
Kwetsbaarheidsscans (KS&R)	✓ Aantal assets / IP's / VM's per scan ✓ Frequentie scans (wekelijks, maandelijks)	✓ Aantal nieuwe systemen ✓ Complexiteit netwerken
Threat Intelligence (TI)	✓ Vaste prijs per maand of gebruiker	✓ Wijzigingen in dreigingslandschap (gevolg: intensiever gebruik)
Security Advisory / Consultancy	✓ Uurtarief per expertise-niveau	✓ Vraag naar maatwerkdiensten of verandering in dreigingsbeeld
Onboarding / Implementatie	✓ Vaste prijs per dienst of per asset/logbron	✓ Complexiteit aansluiting ✓ Aantal integraties (SIEM, CMDB, etc.)
Opslag van logdata	✓ GB/dag logdata ✓ Retentietermijn (bijv. 30/90/365 dagen) ✓ Type opslag: hot, cold, archive	✓ Toename in logvolume ✓ Veranderde compliance-eisen

<u>Vergelijkbaarheid tussen inschrijvers – aanbevolen standaardisatie:</u>

1. Uniforme categorieën voor logbronnen / assets:
   - Endpoint, firewall, cloud, IAM, etc.
   - Staffels (bijv. 1-100, 101-500) voor voorspelbaarheid
2. Vaste definities voor opslag-eenheden:
   - GB per dag, retentie in dagen/maanden/jaar
   - Split tussen hot / cold storage
3. Standaard SLA-niveaus:
   - 24/7 of 8x5
   - Met vaste kosten per SLA-niveau
4. Bundels of strippenkaarten voor flexibele inzet:
   - Incident response, consultancy, threat hunting, etc.

5. True-up/down afspraken:
   - 1–2 keer per jaar harmonisatie op basis van werkelijk gebruik

<u>Veralgemeniseerd prijsmodel:</u>
A. Vaste componenten (eenmalig of periodiek):
- Onboardingkosten (eenmalig)
- MDR-platform licentiekosten (per asset/logsource)
- SOC-monitoringkosten (per asset / GB logdata / EPS)
- Rapportage & overleg (per periode)
- Incident response (basispakket)

B. Variabele componenten (fluctuerend en verrekenbaar):
- Uitbreiding logbronnen, use cases
- Forensics / incident response beyond package
- Threat hunting / red team inzet
- Integratie van nieuwe systemen
- Extra logopslag (hot/cold/archive)

Prijsdrivers die fluctuatie veroorzaken:
- Aantal assets / logbronnen
- Data volume (GB/day)
- Licentiekosten leveranciers (bv. Microsoft Sentinel)
- Verandering in omgeving (Cloud/OT)
- Aantal incidenten/responstijd
- Wijzigingen in SLA-niveau of servicevraag

Aandachtpunt: neem licentieprijzen optioneel of apart, gezien leverancierswijzigingen.

S18 – [100%] Heeft u een beeld bij het aantal klanten c.q. welke omvang u kan bedienen om de dienstverlening per klant met zekerheid en op kwalitatief niveau te leveren waarop de klant kan vertrouwen? Dit met name in gevallen van incidenten die (nagenoeg) gelijktijdig meerdere klanten raken of kunnen raken.

Men heeft een duidelijk beeld van de schaal en capaciteit waarin zij betrouwbare en kwalitatief hoogwaardige SOC-dienstverlening kunnen leveren — ook bij gelijktijdige of grootschalige incidenten die meerdere klanten tegelijk raken. Zij benadrukken dat hun dienstverlening is ontworpen met schaalbaarheid, continuïteit en kwaliteitsborging als uitgangspunten.

Capaciteitsinrichting en schaalbaarheid - Veel partijen hanteren een schaalbaar SOC-model, waarbij capaciteit flexibel kan worden opgeschaald op basis van klantvraag en incidentvolume. Diverse marktpartijen beschikken over internationale of pan-Europese SOC-structuren met geografisch gespreide locaties, waardoor zij hoge beschikbaarheid en redundantie kunnen waarborgen. In een aantal gevallen wordt expliciet verwezen naar het ontbreken van een harde limiet op het aantal klanten dat kan worden bediend, zolang capaciteitsplanning en SLA's in balans blijven.

Opschaling bij gelijktijdige incidenten **-** Vrijwel alle respondenten hebben maatregelen getroffen om adequaat te kunnen opschalen bij simultane incidenten. Veelgenoemde elementen zijn:
- Flexibele inzet van personeel, waaronder achterwachten, interne CSIRT-teams, engineers of analisten uit andere domeinen.

- Automatisering via SOAR (Security Orchestration, Automation and Response), waarmee false positives en standaardincidenten automatisch worden afgehandeld.
- Prioritering op basis van risicoprofielen en SLA's, waarbij kritieke incidenten voorrang krijgen.
- Gestandaardiseerde playbooks en processen voor snelle en consistente incidentrespons.
- Buffercapaciteit of 'trained reserve' die snel inzetbaar is bij piekbelasting.
- Gebruik van multidisciplinaire teams (red teaming, assurance, consultancy) bij escalatie.

Sommigen geven aan dat zij structureel een capaciteitsbuffer aanhouden of pas nieuwe klanten aannemen als zeker is dat dit de kwaliteit en SLA's niet beïnvloedt.

Monitoring en kwaliteitsborging **-** De dienstverlening is bij de meeste partijen ingericht met continue monitoring van capaciteit, logvolume en workload per klant. Door tenant-isolatie, klantprofielen en geautomatiseerde routing van incidenten blijven individuele klantomgevingen goed beheersbaar, ook bij sectorbrede dreigingen of ketenincidenten.

Overige bevindingen:

- Omvang en volwassenheid verschillen per aanbieder. Grote internationale partijen beschikken over duizenden medewerkers en tientallen Cyber Defense Centers; kleinere of nationale partijen richten zich op beheersbare groei en schaalbaarheid binnen hun operationeel model.
- Geen consensus over absolute aantallen. Hoewel sommige partijen concrete aantallen endpoints of klanten noemen die zij kunnen bedienen (bijv. 150.000+ of miljoenen eindgebruikers), geven andere aan dat dit afhangt van specifieke SLA's, use cases en logvolumes.
- Ervaring met grootschalige incidenten. Een aantal marktpartijen verwijzen expliciet naar eerdere ervaringen met brede dreigingen zoals Log4j, Fortinet-kwetsbaarheden of Exchange-zero-days als bewijs voor hun opschaalcapaciteit.
- Enkele partijen verwijzen naar samenwerking binnen sectoren of koepels, zoals SOC NL, waarbij bij grootschalige incidenten ook gezamenlijk opgeschaald kan worden via resource pooling.
- Sommige partijen noemen specifiek sectorprioritering. Zo stellen enkele leveranciers dat bij een capaciteitsconflict prioriteit gegeven wordt aan klanten uit vitale of kritieke sectoren (bijv. Luchtverkeersleiding boven regionale overheden).

S19 – [95%] Wat acht u een zinvol aantal opdrachtnemers bij deze Raamovereenkomst en waarom? U kunt denken aan aspecten als transactiekosten, transitiekosten (in/exit); concurrentie versus de kans op een opdracht per mini-competitie, etc. …

Overwegend acht men een beperkt aantal opdrachtnemers (3-5 opdrachtnemers) het meest zinvol binnen deze raamovereenkomst. Dit aantal wordt gezien als een goede balans tussen concurrentie, uitvoerbaarheid, beheersbaarheid van transactiekosten en het waarborgen van continuïteit en kwaliteit. Een kleiner aantal opdrachtnemers houdt de minicompetities overzichtelijk en beperkt de administratieve belasting voor zowel deelnemers als opdrachtnemers. Dit voorkomt versnippering en voorkomt dat leveranciers afhaken door een te kleine kans op opdrachten. Het induceert ook hogere betrokkenheid en commitment om structureel investeren in klantkennis, tooling en samenwerking, wat de kwaliteit en stabiliteit van de dienstverlening kan verhogen. Ook brengt het Efficiëntie in transitiekosten (in- en uitstroom): minder leveranciers = minder overdrachtsmomenten = minder coördinatie-inspanningen bij wisselingen of beëindiging van contracten. Tenslotte ziet men snellere en

consistentere kennisdeling. Lessen en best practices uit eerdere trajecten kunnen beter worden hergebruikt bij andere deelnemers als er minder partijen betrokken zijn.

Het voordeel van grotere aantallen (5-7 opdrachtnemers), mits goed beheerd, is de keuzevrijheid voor deelnemers, continuïteit bij uitval van een leverancier, en spreiding van risico's. Wel wordt gewaarschuwd voor mogelijke versnippering bij meer dan 7 opdrachtnemers.

Daar waar 1-2 opdrachtnemers de voorkeur geniet, is het wegens de maximale duidelijkheid in verantwoordelijkheden, minimale versnippering van eigenaarschap en kennis, volledige benutting van schaalvoordelen en efficiëntere samenwerking, snellere respons bij incidenten en minder risico op onderlinge afstemmingsproblemen.

Overige bevindingen;

- *Verschuiving van concurrentie naar samenwerking:* binnen een raamovereenkomst voor kritieke diensten als SOC zou de nadruk moeten liggen op samenwerking (bijv. bij incident response of threat sharing), in plaats van alleen concurrentie. Het stimuleren van onderlinge samenwerking tussen opdrachtnemers (eventueel met KPI's) kan bijdragen aan een robuustere keten.
- *Gebruik van minicompetities kritisch bekeken:* dit proces wordt ervaren als belastend, weinig effectief of zelfs contraproductief binnen het SOC-domein, dat vraagt om snelle, stabiele samenwerking.
- *Afstemming op tooling van deelnemers:* technische compatibiliteit met bestaande tooling (zoals Microsoft E5, EDR- of SIEM-oplossingen) kan een belangrijke factor zijn bij de keuze voor opdrachtnemers. Dit kan implicaties hebben voor het ideale aantal leveranciers (bijvoorbeeld om af te stemmen op verschillende technologische profielen).
- *Ervaring uit andere raamovereenkomsten:* eerdere aanbestedingen, zoals die van VNG of Z-CERT, geven 4 tot 6 opdrachtnemers als werkbaar aantal. Deze referenties kunnen relevant zijn voor de uiteindelijke afweging.

S20 – [100%] Deelnemers mogen gebruikmaken van een zogenaamde CTI-feed die door het Nationaal Cyber Security Centrum (NCSC) beschikbaar wordt gesteld. Deze CTI-feed bevat zogenaamde Indicators of Compromise. Zijn partijen in staat en bereid om:

- deze CTI-feed op te nemen in de Montoring en Detectiesystemen die voor deze dienstverlening worden ingezet?
- Alerteringen (sightings) die door deze CTI-feed ontstaan te delen met Opdrachtgever of een door Opdrachtgever aangewezen partij?

NB: het NCSC bepaalt welke partijen van deze feed gebruik mogen maken. De implementatie bij opdrachtnemer moet zodanig zijn dat men zich aan de aansluitvoorwaarden van het NCSC houdt.

Zowel technisch als organisatorisch is men in staat zijn om de CTI-feed van het NCSC te integreren in hun Monitoring- en Detectiesystemen en sightings conform de NCSC-aansluitvoorwaarden te delen met de opdrachtgever of aangewezen partijen. Veel respondenten beschikken over bestaande integraties en ervaring, werken met gestandaardiseerde platforms (zoals MISP of SIEM-systemen), en bieden daarnaast aanvullende threat intelligence-capaciteiten of workflow-ondersteuning. De implementatie is wel afhankelijk van formele aansluiting van de deelnemer bij het NCSC en correcte mandatering. Ter onderbouwing worden argumenten gegeven die in drie categorieën worden onderverdeeld, te weten:

1. Technische integratiecapaciteit is aanwezig

- Vrijwel alle respondenten kunnen de CTI-feed van het NCSC integreren in hun SIEM-, XDR- of andere Monitoring & Detectieplatformen.
- Veelgenoemde ondersteunde platformen: Microsoft Sentinel, Splunk, Elastic, XSOAR, MISP, TAXII, interne Threat Intelligence Platforms (TIP).
- Sommige partijen hebben dit al operationeel draaien voor bestaande klanten binnen de overheid of vitale infrastructuur.

2. Delen van sightings met opdrachtgever wordt standaard ondersteund

- Sightings worden automatisch of semi-automatisch gedeeld met:
  - De opdrachtgever zelf,
  - Of een door de opdrachtgever aangewezen partij,
  - In sommige gevallen ook rechtstreeks terug naar het NCSC (indien relevant en conform afspraken).
- De meldstructuren zijn ingebed in het incidentmanagementproces of geautomatiseerd via CTI-platforms.

3. Bekendheid met en naleving van NCSC-voorwaarden

- De meesten zijn vertrouwd met de formele aansluitvoorwaarden van het NCSC (bijv. via het Nationaal Detectie Netwerk – NDN).
- De meeste leveranciers werken al met deze feed in de praktijk en hebben processen voor:
  - Correcte afhandeling van vertrouwelijkheid (bijv. via NDA's, verwerkersovereenkomsten),
  - Filtering van alerts op basis van classificatie of gevoeligheid,
  - Verantwoorde opslag en terugkoppeling van informatie.
- Enkele leveranciers bieden ook ondersteuning aan deelnemers bij het aanvragen van NCSC-toegang.

<u>Overige bevindingen:</u>

- Vertrouwelijkheid en deling van informatie: Partijen benadrukken het belang van duidelijke afspraken over welke gegevens wanneer worden gedeeld, met wie, en onder welke voorwaarden.
- Versnippering voorkomen: Bij meerdere securityleveranciers in een ecosysteem is het belangrijk om te voorkomen dat sightings dubbel worden gemeld, of juist niet worden opgepakt door onduidelijkheden over rollen/verantwoordelijkheden.
- Mogelijkheid tot foutieve interpretatie van IoC's: Sommige partijen waarschuwen dat niet elke indicator per definitie leidt tot een dreiging; juiste interpretatie binnen context is belangrijk om false positives te beperken.

S21 – [100%] In hoeverre speelt AI een rol in uw dienstverlening?

AI is algemeen geaccepteerd en breed ingebed in SOC/MDR-diensten. Veel respondenten erkennen dat AI tegenwoordig een cruciale rol speelt in hun Security Operations Center- of Managed Detection & Response-diensten. AI wordt ingezet om snelheid, schaalbaarheid, efficiëntie en consistentie te verhogen, met behoud van kwaliteit en betrouwbaarheid.
AI speelt bij vrijwel alle respondenten een belangrijke rol binnen SOC- en MDR-diensten, voornamelijk om detectie, triage, automatisering en threat intelligence te versterken. AI is geïntegreerd in kernprocessen, platformen en tooling en fungeert als cruciaal instrument voor snelheid, schaalbaarheid en kwaliteit. Ondanks de variatie in volwassenheid, blijft menselijke controle essentieel, waarbij AI zoveel mogelijk transparant, uitlegbaar en gecontroleerd wordt

ingezet. De meeste leveranciers anticiperen actief op toekomstige AI-ontwikkelingen en bieden hiermee een technologisch toekomstbestendige dienstverlening. Actuele relevante toepassing van AI:

- *Gedetecteerde anomalieën & agressieve dreigingen:* AI/ML-systemen signaleren afwijkend gedrag, zero-day-bedreigingen en detecteren weak signals die anders ongezien blijven.
- *False positive reductie & alert triage:* AI minimaliseert ruis en vermindert alert fatigue, zodat analisten zich kunnen richten op relevante incidenten.
- *Threat intelligence correlatie & predictive modeling:* AI versnelt matching met externe intelligence-feeds (zoals NCSC), maakt trendanalyses en voorspellingen van potentiële risico's mogelijk.
- *Generative en agentic AI voor ondersteuning:* AI-tools helpen bij natuurlijke taalzoekopdrachten, samenvatting van incidentgegevens, case-overzichten en voorgestelde responsacties. Deze systemen ondersteunen op een gecontroleerde manier (human-in-the-loop), met transparantie, controleerbaarheid en uiteindelijke menselijke validatie.
- *Incidentmanagement & workflowautomatisering:* Agentic AI voert autonome taken uit zoals alert-correlatie, case-samenvatting en response-acties binnen een Secure-by-Design-framework.

<u>Variatie in volwassenheid en ambitie:</u>

- Sommigen maken slechts gebruik van basis AI/ML-functies binnen SIEM of SOAR.
- Anderen experimenteren met generatieve AI of LLMs, of hebben pilots lopen met tools zoals Microsoft Security Copilot.
- Sommigen zijn terughoudend (bijv. ten aanzien van generatieve AI) vanwege risico's zoals hallucinations, maar blijven technologische ontwikkeling wel volgen en voorbereiden op toekomstig gebruik.
- Toepassing van AI vindt plaats in gecontroleerde omgevingen, vaak met interne AI-policies en -frameworks om verantwoord gebruik te garanderen.

Human-in-the-loop - Bij vrijwel alle respondenten versterkt AI de menselijke rol en vervangt deze niet. Menselijke analisten blijven verantwoordelijk voor de uiteindelijke beoordeling, validatie van AI-suggesties en besluitvorming. Dit waarborgt transparantie, uitlegbaarheid en controle, in lijn met de Europese AI-wetgeving (zoals de AI Act en secure-by-design principes).

S22 – [100%] Welke impact verwacht u van de eisen die voortvloeien uit de invoering van de EU AI-verordening en verwacht u dat u hieraan kunt voldoen?

De meeste respondenten verwachten significante impact van de EU AI-verordening, vooral voor AI-toepassingen in SOC/MDR-diensten met hoog risico. Tegelijkertijd is het algemene beeld dat leveranciers goed voorbereid zijn om hieraan te voldoen. Vrijwel alle partijen hanteren al principes van Responsible AI, met aandacht voor transparantie, uitlegbaarheid, menselijke controle en auditbaarheid. Verschillen bestaan in maturiteit en in de mate waarin AI nu al operationeel wordt ingezet. De AI-verordening wordt gezien als een noodzakelijke en zelfs wenselijke normstelling die de kwaliteit van dienstverlening versterkt, met de meest merkbare of aanzienlijke impact wanneer AI-systemen worden ingezet voor Monitoring & Detectie (M&D), geautomatiseerde dreigingsanalyse, en besluitvorming binnen cybersecurityprocessen. Voor deze toepassingen geldt doorgaans het "hoog risico"-regime binnen de AI-verordening, wat leidt tot extra verplichtingen op het gebied van transparantie

en uitlegbaarheid van AI-systemen; menselijk toezicht op AI-besluiten; documentatie- en auditvereisten; risicoanalyse en mitigatie; beveiliging en toegangscontrole.
Ook wordt impact verwacht op organisatorisch vlak, bijvoorbeeld in governance, compliance, en het aantoonbaar kunnen maken van verantwoorde inzet van AI.
Daarentegen geven anderen aan dat de impact beperkt zal zijn, omdat hun AI-toepassingen als laag risico worden ingeschat; zij slechts beperkt gebruikmaken van AI (bijv. alleen ML voor gedragsanalyse); of omdat generatieve AI nog niet operationeel wordt ingezet, vanwege zorgen over betrouwbaarheid.

Alle respondenten verwachten te kunnen voldoen aan de AI-verordening (althans, niemand beweert het tegendeel), dan wel dat zij daar al grotendeels aan voldoen. Meest genoemd in dit verband het al toepassen van "human-in-the-loop" of menselijke validatie van AI-uitvoer, bestaande maatregelen op het gebied van uitlegbaarheid, logging, auditability en risicobeoordeling of het volgen van een stapsgewijze aanpak om tools en processen in lijn te brengen met de verordening. Anderen geven aan dat zij nog bezig zijn met voorbereiding, zoals het classificeren van hun AI-systemen of het aanpassen van interne procedures en documentatie. Dit geldt met name voor leveranciers die verwachten dat hun AI-componenten (nog) niet onder het "hoog risico"-regime vallen, maar die wel anticiperen op toekomstige aanpassingen.

S23 – [95%] Heeft u een visie of activiteiten op het gebied van Quantum Veilige Cryptografie en welk effect dit op (de kwaliteit van) uw dienstverlening heeft? U hoeft geen uitgebreide visie op dit onderwerp zelf te geven. U kunt zich beperken tot highlights en relevante punten voor inbedding in een aanbesteding.

Een aantal respondenten beschikt over een duidelijke concrete QVC-strategie. Anderen bevinden zich in een voorbereidende of onderzoekende fase. Enkelen geven aan (nog) geen zelfstandige visie te hebben, maar erkennen wel het belang van QVC. Het strategische belang van Quantum Veilige Cryptografie (QVC) voor de toekomst van cybersecurity wordt aldus breed herkend. Men anticipeert op de impact van quantumcomputers op bestaande encryptiestandaarden en treffen voorbereidingen voor de migratie naar post-quantum cryptografie (PQC). De bestaande visies of activiteiten richten zich op:

- *Crypto-agility*: architecturen en diensten worden voorbereid op het flexibel kunnen vervangen van cryptografie.
- *Risico-inventarisatie*: inventarisatie van kwetsbare systemen en datastromen die vatbaar zijn voor "store now, decrypt later"-aanvallen.
- *Standaarden*: het volgen actief de ontwikkelingen bij o.a. NIST, ETSI en TNO.
- *Bewustwording*: ondersteunen van klanten met bewustwordingssessies, assessments, transitie-roadmaps en advies over QVC.
- *Samenwerking*: er wordt samengewerkt met technologiepartners die PQC integreren in hun producten (zoals Microsoft, Cisco, Fortinet).

<u>Concrete implementaties en initiatieven:</u>

- *Cryptoregistratie*: sommigen nemen een actieve rol in het registreren van huidige cryptografie als voorbereiding op migratie (conform richtlijnen van TNO en de EU).
- *Monitoring & detectie*: en SOC-diensten wordt nagedacht over de impact van sterkere encryptie op decryptiemogelijkheden bij monitoring. Oplossingen zoals agents of alternatieve databronnen worden ingezet.
- *Gebruik van PQC-primitieven*: enkelen werken al met HSM's en cryptobibliotheken die ondersteuning bieden voor PQC.

- *Quantum Key Distribution (QKD)*: er zijn Proof-of-Concepts met QKD opgezet en samenwerking met academische instellingen, zoals de TU Eindhoven.
- *Geen negatieve impact op dienstverlening*: de meesten geven aan dat QVC geen negatieve gevolgen heeft voor de kwaliteit van hun dienstverlening. In enkele gevallen worden mogelijke compatibiliteitsproblemen met verouderde hardware genoemd. Sommigen achten de impact op hun M&D- en kwetsbaarheidsscandiensten beperkt.

S24 – [95%] Ingeval een deelnemer van een eigen SOC gebruikmaakt en ook SOC-diensten binnen de raamovereenkomst wenst af te nemen, ontstaat er een hybride samenwerkvorm met een opdrachtnemer. Welke randvoorwaarden of aandachtspunten zou u hierbij willen meegeven, naast het logischerwijs goed afbakenen van de verantwoordelijkheden en bevoegdheden?

De meeste respondenten geven aan ruime ervaring te hebben met hybride SOC-modellen en beschouwen deze als goed uitvoerbaar, mits zorgvuldig ingericht. Dat houdt in dat naast een heldere afbakening van verantwoordelijkheden en bevoegdheden er regelmatige afstemming en gezamenlijke procesvoering nodig is. Daarnaast dienen partijen bereid te zijn tot samenwerking op basis van wederzijds vertrouwen, standaardisatie en gedeelde doelstellingen. Meer specifiek worden de volgende randvoorwaarden en aandachtspunten veelvuldig genoemd:

- *Governance en rolverdeling*
  - RACI-model: Heldere vastlegging van wie verantwoordelijk is voor welke taken (detectie, triage, respons, escalatie).
  - Incident eigenaarschap: Per incidenttype moet duidelijk zijn wie 'in the lead' is.
  - Fallback-afspraken: Voor situaties waarin onduidelijkheid of geschil ontstaat over de verantwoordelijkheid.
  - SLA's & KPI's: Duidelijke meet- en prestatieafspraken, afgestemd op de hybride context.
- *Afstemming van processen en procedures*
  - Use cases & rule sets: Gezamenlijke ontwikkeling, tuning en onderhoud van detectieregels.
  - Detectie- en responsdraaiboeken: Harmonisatie van werkinstructies en playbooks.
  - Escalatieprocedures: Uniforme en vooraf vastgestelde escalatiestappen.
  - Change/configuratiebeheer: Wijzigingen in de IT-omgeving of detectie-instellingen moeten gedeeld worden.
- *Technische integratie en tooling*
  - Gedeelde zichtbaarheid: Toegang tot logdata, alerts, SIEM-dashboards, threat intelligence en incidentstatussen.
  - Toegangsbeheer: Rolgebaseerde toegang tot tooling en data (need-to-know).
  - Interface-koppelingen: Technische integraties tussen systemen zoals SIEM, SOAR, CMDB en ticketingtools.
  - Toolcompatibiliteit: Afspraken over gebruik van dezelfde tooling of onderlinge koppeling (soms verplicht gebruik van specifieke tooling zoals Exabeam of Sentinel)
- *Samenwerking en communicatie*
  - Reguliere overleggen: Operationeel (dagelijks), tactisch (wekelijks/maandelijks), strategisch (kwartaal).
  - Gezamenlijke incidentbesprekingen: Bijvoorbeeld bij complexe of multiparty-incidenten.

- Realtime communicatiemiddelen: Beveiligde chat, gedeelde dashboards, geïntegreerde ticketsystemen.

- *Verdieping en kennisdeling*
  - Purple teaming: Gezamenlijke oefeningen om detectie, respons en samenwerking te verbeteren.
  - Kennisoverdracht: Van externe specialisten (L3, threat hunting, malware reverse engineering) naar interne teams.
  - Gebruik maken van specifieke expertise: Bijv. inzet van externe forensische specialisten of ondersteuning bij dreigingsmodellering.
- *Kwaliteit en compliance*
  - Gedeelde rapportages: Geconsolideerde dashboards en performance-overzichten.
  - Security & compliance: Uniforme afstemming over audittrails, datatoegang, NIS2-rapportages en meldstructuren.
  - Gebruik van standaardframeworks: Sommige partijen hanteren frameworks zoals SOC-NL of eigen gestandaardiseerde samenwerkingsmodellen.
- *Kritische kanttekeningen*

  Een aantal partijen wijst op risico's en beperkingen van hybride modellen:
  - Complexere SLA-meetbaarheid: Door gedeelde verantwoordelijkheid.
  - Hogere kosten: Door dubbele bezetting en technische integratie-inspanningen.
  - Communicatie-overhead: Door verschillen in werkwijze en cultuur.
  - Minder efficiëntie**:** Vooral wanneer het interne SOC onderbenut raakt.

S25 – [100%] In hoeverre is het dienstverleningsconcept (met het startpakket en aanvullende diensten verenigbaar) met een hybride SOC-variant waarin de deelnemende dienst zelf tijdens kantoortijden voorziet in M&D dienstverlening en de leverancier zorgt voor de bewaking daarbuiten. Is een dergelijk model hanteerbaar en welke specifieke aandachtspunten en randvoorwaarden stelt dit?

Overwegend achten respondenten een dergelijk hybride SOC-model hanteerbaar, mits zorgvuldig geborgd met duidelijke afspraken, governance en technische integratie. Er bestaat echter ook kritische nuance: sommige partijen adviseren eerder een taakgerichte indeling in plaats van tijdsplanning, of noemen contextverlies en operationele complexiteit als risico's. er is nochtans brede consensus over onderstaande randvoorwaarden en aandachtspunten:

1. Governance en verantwoordelijkheden
   - Heldere rolverdeling (RACI): wie is 'lead' bij detectie, triage, escalatie en respons - ook buiten kantooruren.
   - Overdrachtsregeling ('shift handover'): tijdige, volledige overdracht van incidentcontext, acties en status.
   - Eenduidige escalatie- en communicatielijnen, inclusief fallback bij onduidelijkheid.
   - Lokale ondersteuning en mandatering: contactgegevens van crisisteamleden, toegang tot portalen, en beslissers binnen de deelnemer.
2. Consistentie in detectie, tooling en processen
   - Gedeelde tooling: uniforme toegang tot SIEM, SOAR, dashboards, logdata en tickets.
   - Afstemming van detectieregels en playbooks: beide partijen werken met dezelfde use cases, tuning en guidelines.
   - Procesharmonisatie: triage-, escalatie- en verantwoordingsprocessen moeten naadloos aansluiten, ongeacht tijd.
3. Continuïteit en kwaliteit van dienstverlening
   - Doorlopende contextkennis: een gedeeld model (klant én leverancier tijdens kantooruren) kan kennisdeling bevorderen.

- Processen voor overdracht en follow-up bij incidenten: zowel real-time handling als opvolging tijdens kantooruren.
- Rapportage en SLA-structuren: heldere afspraken over responsetijden, KPI's en verantwoordelijkheid per shift.

4. Risico's en beperkingen
   - Kennisverlies bij tijdscheidingen: analisten missen cruciale context en kunnen patronen missen (hoge false positive kans).
   - Verhoogde complexiteit: meer communicatie, afstemming en technische koppelingen betekenen grotere organisatorische druk en kosten.
   - Beperktere efficiëntie: gebrek aan continuïteit en context kan leiden tot vertraagde respons of onvolledige afhandeling.
5. Alternatieve aanpak: op taakniveau indelen
   - Enkele partijen adviseren, in plaats van op tijd, een structuur op basis van de rolverdeling in het SOC (tier-structuur):
     - Tier 1/2 (monitoring & triage): door leverancier
     - Tier 3 (diepgaande analyse, besluitvorming): bij deelnemer

Dit model waarborgt consistentie, contextbeheer en meetbaarheid, en minimaliseert risico's op blinde vlekken en wisselingsverlies.

S26 – [95%] In hoeverre is het dienstverleningsconcept (met het startpakket en aanvullende diensten) verenigbaar met een hybride SOC-variant waarin de deelnemende dienst bepaalde M&D-diensten afneemt van een rijksinterne dienstverlener (SSC of anderszins) en de leverancier zorgdraagt voor additionele diensten en/of verhoging van de dekkingsgraad. Is een dergelijk model hanteerbaar en welke specifieke aandachtspunten en randvoorwaarden stelt dit?

Het overgrote deel geeft aan dat een hybride SOC-model technisch en organisatorisch goed hanteerbaar is, mits er duidelijke afspraken worden gemaakt over taakverdeling, governance, communicatie en technische integratie. Het dienstverleningsconcept met een startpakket en aanvullende diensten sluit volgens veel partijen aan op een dergelijke hybride opzet, juist vanwege de modulaire en flexibele opbouw. Velen hebben ervaring met situaties waarin de basis-SOC-dienstverlening bij een interne dienstverlener ligt, en zij aanvullend optreden voor bijvoorbeeld verdiepende analyse, detectieverbetering of incident response. Dergelijke hybride modellen worden als steeds gebruikelijker beschouwd. Belangrijke voorwaarden voor een werkbaar hybride SOC-model zijn:

- Heldere rol- en verantwoordelijkheidsverdeling:
  - Duidelijk maken welke partij verantwoordelijk is voor welke componenten van detectie en response.
  - Aandacht voor overlappende verantwoordelijkheden en het voorkomen van blinde vlekken of dubbel werk.
  - Gebruik van tools als RASCI-matrixen wordt aanbevolen.
- Effectieve governance en regievoering:
  - Eén partij dient eindverantwoordelijkheid te dragen voor regie, coördinatie bij incidenten en het doorlopen van playbooks.
  - Escalatieprocedures en communicatiekanalen moeten vooraf helder zijn vastgelegd.
- Technische integratie:
  - Koppelingen tussen SIEM, XDR, ticketing en threat intelligence moeten technisch mogelijk zijn.
  - Uniformiteit in logformaten, dashboards en rapportages bevordert samenwerking.

- Toegang tot relevante data:
  - Beide partijen moeten (gedeeltelijk) toegang hebben tot dezelfde logbronnen en monitoringdata om effectief te kunnen samenwerken.
  - Datafeeds of gestandaardiseerde informatie-uitwisseling kunnen hierin voorzien.
- Compliance en juridische borging:
  - Afstemming over naleving van AVG, BIO, NIS2 en andere relevante normen.
  - Juridische afspraken rondom verantwoordelijkheden, geheimhouding en toezicht (bijv. audittrail).
- Kwaliteitsborging:
  - Afspraken over KPI's, SLA's en gezamenlijke evaluaties zijn essentieel voor het borgen van kwaliteit in een hybride setting.
- Use case-gebaseerde taakverdeling:
  - Verdeling van taken gebaseerd op risicoprofiel, kritikaliteit van assets en beschikbaarheid van expertise.

<u>Overige bevindingen:</u>

- Hybride modellen komen in de praktijk regelmatig voor, bijvoorbeeld bij klanten die al bestaande SOC-dienstverlening afnemen van een SSC of andere interne dienstverlener.
- Er wordt gewezen op de technische complexiteit binnen het Microsoft-ecosysteem, waar gedeelde verantwoordelijkheden de effectiviteit kunnen verlagen als configuraties niet goed op elkaar zijn afgestemd.
- Bepaald activiteiten, zoals specialistische taken (threat hunting, malware-analyse, forensisch onderzoek,…), passen vaak beter bij een externe leverancier, terwijl basismonitoring bij een interne dienstverlener kan blijven.
- Escalatie en overdrachtsprocedures ten behoeve van een duidelijke shift-overdracht, gedeeld incidenteigenaarschap en goed afgestemde playbooks bij gedeelde incidentafhandeling.
- Gebruik standaarden als MITRE ATT&CK, NIST of het SOC NL-framework voor structuur en harmonisatie van processen.
- Naast de SLA is ook contractuele borging van de Operational Level Agreements (OLA's) tussen de betrokken partijen belangrijk voor het managen van onderlinge afspraken.
- De effectiviteit kan mede afhankelijk zijn van de samenwerking met de eventuele Nederlandse rijksinterne dienstverlener. Dit kan variëren per situatie.

S27 – [90%] Zijn er voor deelnemers nog niet benoemde randvoorwaarden van belang bij de afname van deze diensten, zoals een relatie met de (eigen en/of externe) SOC die monitoring- en detectiediensten uitvoert?

De meeste respondenten geven aan dat er aanvullende randvoorwaarden kunnen gelden bij de afname van Monitoring- en Detectiediensten (M&D), vooral in situaties waarin de deelnemer reeds gebruikmaakt van een eigen of externe SOC. Deze aanvullende voorwaarden zijn doorgaans gericht op het borgen van effectieve samenwerking, integratie en procesafstemming. De kernboodschap is, dat de effectiviteit van de dienstverlening in een dergelijk model sterk afhankelijk is van duidelijke afspraken over taken, informatiestromen, technische koppelingen en governance. Hierbij speelt ook de volwassenheid van de deelnemer op het gebied van IT en security een belangrijke rol:

- Samenwerking en interfacing met bestaande SOC's:
  - Afspraken over logdeling, datatoegang, tooling-integraties (zoals SIEM of scanners) en procesuitlijning zijn cruciaal.

- Governance-afstemming is vereist wanneer meerdere partijen in de detectieketen actief zijn.
- Heldere verantwoordelijkheidsverdeling:
  - Wie is leidend bij triage en incidentafhandeling?
  - Wie implementeert mitigaties en opvolgmaatregelen?
- Structurering via contractafspraken:
  - Verschillende partijen stellen voor om een master agreement op te nemen in de raamovereenkomst (ROK), met per deelnemer een Statement of Work (SoW) voor de specifieke scope, rollen en verwachtingen.
- Afstemming van processen:
  - Incidentmanagement, escalatie- en crisisprocessen moeten op elkaar zijn afgestemd.
  - Dit voorkomt vertragingen, miscommunicatie en dubbele opvolging.
- Beschikbaarheid van relevante gegevens en middelen:
  - Toegang tot logbronnen, testomgevingen en actuele assetinformatie.
  - Technische documentatie en contactpersonen aan de kant van de deelnemer zijn nodig om integratie te versnellen.
- Personele en organisatorische volwassenheid:
  - Deelnemers moeten beschikken over voldoende interne capaciteit, eigenaarschap en bereidheid tot samenwerking.
  - Een gezamenlijke volwassenheidstoets aan het begin van de samenwerking wordt als nuttig ervaren.
- Security-specifieke randvoorwaarden:
  - Juridische aspecten zoals vrijwaring bij monitoring.
  - Classificatie van data.
  - Integratie van threat intelligence, inclusief IOCs, TTPs en feedback loops.

<u>Overige bevindingen:</u>

- Structuur met Master Agreement en SoW: een master agreement op raamcontractniveau met per deelnemer een Statement of Work. Deze structuur biedt flexibiliteit én duidelijkheid.
- Organisatorische volwassenheid van deelnemer: de effectiviteit van de dienstverlening is mede afhankelijk van de volwassenheid van de deelnemer op het gebied van securityprocessen, tooling en samenwerking. Dit vraagt soms om initiële procesaanpassingen of begeleiding.
- Beperking bij Microsoft-licenties: een technische randvoorwaarde: deelnemers zonder Microsoft E5-licentie kunnen wel deelnemen, maar met een beperktere scope.
- Escalatie en incidentafhandeling: Het belang van een duidelijk geëigend incidentmanagement- en escalatieproces aan de zijde van de deelnemer wordt nadrukkelijk genoemd, inclusief afstemming met het proces van de leverancier.
- Federatieve SOC-inrichting: de mogelijkheid van een federatief SOC-model, waarin samenwerking plaatsvindt tussen meerdere SOC's (intern en extern). Dit geeft wel de noodzaak tot aanvullende werkafspraken vanwege de complexiteit.

S28 – [100%] In bijlage 4 bij dit document treft u een conceptversie van het programma van eisen aan. Wat vindt u van de voorliggende conceptversie van het programma van eisen?
Bij uw beantwoording gaat u bij voorkeur in op de volgende subvragen:

a. Welke eisen moeten naar uw mening vervallen of afgezwakt worden om te voorkomen dat u en/of andere potentiële inschrijvers hier niet aan kunnen/willen voldoen (verlagen instapniveau)? Motiveer uw antwoord.

b. Welke eisen moeten naar uw mening nog toegevoegd of strikter gesteld worden om risico's voor Deelnemers te beperken/minimaliseren (verhogen instapniveau)? Motiveer uw antwoord.

Welke andere suggesties wilt u doorgeven?

Men is overwegend positief en vindt het PvE over het algemeen goed gestructureerd en grotendeels uitvoerbaar. Wel wordt opgemerkt op dat sommige eisen te strikt, te specifiek of onduidelijk zijn, en dat deze aanpassingen behoeven om onnodige belemmeringen te voorkomen.

Subvraag	Thema	Belangrijkste opmerkingen
a. Verlagen instapniveau	Taal, certificering, tooling, toegang, deadlines	Minder strikte eisen rond taalgebruik, verplichte tools, toegang tot data, individuele certificaten en incidentdeadlines
b. Verhogen instapniveau	24/7 monitoring, AI, compliance, onboarding, OT	Meer aandacht voor 24/7 aanwezigheid, inzet AI, duidelijke onboarding, robuuste compliance en future-proofing (OT, hybride SOC)
Overige suggesties	PvE-verduidelijking, hybride samenwerking, innovatie	Verbeter terminologie en structuur PvE, geef ruimte voor innovatie, en richt samenwerking in hybride modellen goed in

<u>Eisen die moeten vervallen of afgezwakt worden (verlaging instapniveau):</u>

- *Taal- en rapportage-eisen* - Verplichte Nederlandse taal voor alle communicatie beperkt internationale inzetbaarheid. Advies: eis beperken tot Nederlandstalige rapportages of klantcontactmomenten.
- *Certificering en kwalificaties* - b4.7 [beveiligingsmaatregelen]: Verplichte certificaten zoals CISSP/CEH/OSCP per functie zijn te beperkend; Focus op aantoonbare bekwaamheid of teamcertificering; laat ruimte voor gelijkwaardigheid.
- *Tooling en formats* - Verplichte tooling of formats beperken maatwerk: Bijvoorbeeld vaste dashboards, SIEM-inrichting, rapportage-indelingen. Advies: Laat ruimte voor eigen inrichting binnen functionele eisen.
- *Logdata en datatoegang* - Verplichte toegang tot volledige security log data lake: juridisch en operationeel niet wenselijk. Advies: Beperk scope tot noodzakelijke logbronnen, bij voorkeur via API's. Pas op met het gebruik van specifieke proprietary technologieën (B4.44); dit kan flexibiliteit beperken en kosten verhogen.
- *Toegangsbeperkingen* - eisen m.b.t. "need-to-know" (B4.4, B4.26 en B4.41) niet te strikt toepassen omdat dit belemmerend kan zijn in de samenwerking.
- *Testverantwoordelijkheden* - Pentestverantwoordelijkheid moet beperkt zijn tot eigen infrastructuur. Advies: Verduidelijk reikwijdte van verplichtingen en leg de nadruk op assurance en rapportage.
- *Gebruik van Microsoft-licenties* - B4.11: Onduidelijkheid over gebruik van Microsoft Sentinel/E5-licenties leidt tot risico's op meerkosten.
- *Rapportage- en RCA-deadlines* - Deadlines van 24/72 uur bij incidenten zijn soms niet haalbaar. Advies: Gebruik "best effort" formulering, afhankelijk van toegang tot benodigde data.

<u>Onduidelijke of verwarrende eisen</u>

- A,5,4g [*TLP-codering*]: niet duidelijk wat wordt bedoeld of op welke wijze inschrijver aan de labeling-eisen moet voldoen.
- Eisen zoals B4.53 (onboarding vs. implementatie),
- B4.48 (overdracht detectieregels), en B4.51 (prioriteringsmatrix) zijn onduidelijk of onrealistisch.

<u>Eisen die moeten worden toegevoegd of aangescherpt (verhoging instapniveau):</u>

- *24/7 monitoring en respons*
  - Permanente bemensing SOC (eyes-on-screen) i.p.v. enkel alerting is belangrijk.
  - De escalatie- en fallbackprocedures moeten robuust zijn met goed gestructureerde communicatie en bij voorkeur een integratie met het ticketsysteem.
  - B4.27 [verzamelen forensische informatie]: Eisen m.b.t medewerking specifieker maken. Meekijken (op afstand) is akkoord; autonoom toegang/inzage in systemen die door Opdrachtnemer worden beheerd is <u>niet</u> akkoord.
- *Informatiebeveiliging & compliance*
  - Strengere eisen voor fysieke/logische beveiliging.
  - Logintegriteit, chain-of-custody, cryptografische signing bij logdata.
  - Alleen versleutelde communicatie, gebruik MFA/jump hosts, tenant separation.
- *Slimmere technologie & AI*
  - Verplichte inzet van AI/ML voor triage, scoring, anomaly detection.
  - Integratie met MITRE ATT&CK.
- *Kennisopbouw en onboarding*
  - Minimale eisen aan onboarding: intake, contextanalyse, use case bibliotheek.
- *Gebruik en actualisering van Use Cases*
  - Regelmatig onderhoud en updates van detectieregels verplicht stellen.
- *Ervaring met gevoelige overheidsdata*
  - Strenge eisen bij AMarktpartij-3-projecten: screening personeel, bewezen overheidsprojecten, data-opslag in NL/on-premise.
- *OT-monitoring en future-proofing*
  - Monitoring van OT-systemen toevoegen aan de scope.
  - Verwerk ook trends zoals hybrid SOC, purple teaming en dreigingsmodellering.
- *Duidelijkheid en verifieerbaarheid*
  - Voeg expliciete certificeringseisen toe aan auditrapporten: ISO 27001, ISAE3400 D, door externe partij.
  - Striktere formulering eisen rond logverwerking gekoppeld aan GB/dag en bewaartermijn i.p.v. aantal assets.

<u>Overige suggesties en adviezen:</u>

- V*erbeter PvE-structuur en begripsgebruik*
  - Duidelijk onderscheid tussen "basis M&D", "aanvullend M&D" en "kwetsbaarheidsscanning".
  - Heldere definities voor "implementatie", "onboarding" en "adequaat".
- *Hybride samenwerking en governance*
  - Stel richtlijnen op voor samenwerking met andere SOC-partijen (bijv. Azure Lighthouse).
  - Eisen over shiftwissels, ticketoverdracht, incident-eigenaarschap.
- *Innovatie & differentiatie*
  - Laat ruimte voor innovatieve invulling (bijv. AI, behavior-based detection).
  - SLA's en responstijden differentiëren per dienst of risicoprofiel.
- *Formatvoorstellen van marktpartijen*
  - Enkele marktpartijen leverden bijlagen aan (SLA's, DAP's, deliverables).

S29 – [70%] Hieronder is ruimte voor uw eventuele aanvullende reactie

- Overweeg End-to-End Threat Management toe te voegen
- Toevoegen van elementen die bijdragen aan continu verbeteren zoals Maandelijks contentverrijking; Threat Intelligence Integratie.
- Als Deelnemer al over een SIEM beschikt, kan een minicompetitie (altijd) als vrijblijvend worden uitgevraagd.
- Sluit licentiekosten uit van de Social Return eis/waarde.
- Sta verschillende manieren van afrekenmodellen toe, omdat er in de markt verschillende prijsmodellen zijn.
- Verlangen naar samenwerking op basis van gedeelde waarden en vertrouwen.
- Pleidooi voor realistische eisen en maatwerk in KPI's en contractstructuur; stel KPI's per perceel op en niet generiek over het gehele contract. Eén partij geeft aan dat het voorgestelde gele kaarten systeem minder geschikt is voor SOC-diensten.
- Eis AP.12 (eisen aan offertes) worden als ongeschikt gezien voor SOC-diensten.
- Beperking afhankelijkheid van Big Tech / Microsoft; Enkele respondenten pleiten voor technologische diversiteit (bijv. Splunk, Exabeam), beperken lock-in, waarborgen gegevenssoevereiniteit.
- Post-Quantum voorbereiden op het verwerken van threat intel gerelateerd aan cryptoregistratie en kwetsbare algoritmes, in lijn met het TNO-handboek en EU-tijdlijnen.
- AI-verantwoording dat de inzet voor detectie/triage aan de eisen conform EU AI-verordening.
- Security Maturity Assessments; Eén marktpartij stelt dit voor als periodieke evaluatieverplichting.
- SOC-diensten zoveel mogelijk in standaardtarief opnemen (voorkomen verrassingskosten);
- Alternatieve prijsmodellen (niet alleen op basis van GB/dag)
- Beperking van generieke eisen zoals A.5; welke eisen zijn écht van toepassing op SOC-diensten. Zo is de vraag in hoeverre de eisen uit NORA en Forum Standaardisatie van toepassing zijn op SOC-diensten.
- Beperkte geschiktheid van AP.12 (CV's en methodieken) voor SOC-aanbesteding. Er zijn alternatieven voor op basis van oplossingen en processen.

3.4 Overige IB-diensten

OIB1 – [100%] Op welke verschillende onderwerpen (zoals genoemd in de sub paragrafen) van de Overige IB-diensten kunt en wilt u wel/geen diensten leveren?

Er is een mix van full-service providers en nichepartijen. Een dekkend aanbod veelal in samenwerking met anderen c.q. onderaannemers. Het merendeel van de respondenten (ca. 14 van de 23) geeft aan alle genoemde IB-diensten te kunnen leveren. Enkelen beperken zich tot specifieke onderdelen. Sommigen leveren Threat Intelligence niet als separate dienst. Anderen leveren wel separate diensten voor CTI-datafeeds als maatwerk, niet als schaalbare (standaard) dienst. Dit laatste is ook door enkelen genoemd met betrekking tot (Social) Awareness.

Incident Response & Forensisch Onderzoek is vaak gekoppeld, met nadruk op multidisciplinaire aanpak en juridische borging.
(Social) Awareness vaak ingericht via e-learning, phishing simulaties of gedragsprogramma's.
Threat Intelligence/Datafeed heeft meestal koppelingen naar/met externe feeds (o.a. NCSC) en/of via partners.

OIB2 – [90%] Wat is uw advies over het wel of niet als geclusterd geheel aanbesteden van de Overige IB-diensten? Welke onderwerpen zouden beter niet/wel geclusterd kunnen worden aanbesteed c.q. opgenomen in dezelfde (raam)overeenkomst? Waarom?

Ruim de helft van de respondenten waarschuwt tegen een het in één geheel samenvoegen van de Overige IB-diensten. Daarvoor zijn de genoemde diensten te divers. Meerdere partijen pleiten voor gedeeltelijke clustering:

- IR, FO en TI samen (operationeel en urgent).
- Awareness en consultancy apart (strategisch en planbaar).

Een aantal respondenten vindt dat alle onderdelen apart moeten worden aanbesteed, zodat specialisten beter kunnen inschrijven en kwaliteit behouden blijft.
Een minderheid ziet vooral voordelen in het bundelen van diensten omdat het een integrale benadering mogelijk maakt, synergie en schaalvoordelen kan brengen. Er bestaat bij clustering wel een mogelijk risico dat nichepartijen/specialisten feitelijk worden uitgesloten.
Een verstandige keuze van clustering houdt in ieder geval rekening met de verschillende urgentieprofielen (24/7 vs. projectmatig) en vermijdt afhankelijkheden tussen percelen (zoals bijvoorbeeld Threat Intelligence in relatie met Red teaming).

OIB3 – [20%] Hieronder is ruimte voor uw eventuele aanvullende reactie ten aanzien van de mogelijke clustering van inkoopbehoeftes op het gebied van de 'overige IB-diensten'

Er zijn een beperkt aantal aanvullingen, die vooral de voorkeur voor scheiding of beperkte clustering bevestigen:

- Elk onderwerp apart aanbesteden vanwege uiteenlopende benodigde kennis, eisen en risico's.
- Incident Response vergt specifieke stand-bycapaciteit met een eigen prijsmodel (financiering vooraf). Zowel qua dynamiek als pijsmodel is het beter deze niet samen te voegen met minder urgente diensten.
- Bepaalde diensten ontbreken:
  - dienstverlening gerelateerd aan Identity & Access-management, inclusief Privileged Access Management (onderzoeken Programma van Eisen, definitie scenario's e.d.)
  - dienstverlening gerelateerd aan security architectuur in bredere zin (zowel het opstellen als het reviewen van security).

3.4.1 Incident response

IR1 – [100%] Herkent u bovenstaande indeling in uw producten/diensten portfolio?
a. Zijn de diensten bij u als zodanig georganiseerd/ingericht, dan wel andere samenstellingen of dwarsverbanden?

b. Wat kunt u meegeven als belangrijke zaken met betrekking tot verantwoordelijkheden en activiteiten binnen een ter zake contract?

Ad a. - De overgrote meerderheid respondenten herkent de geschetste indeling. Velen geven aan dat hun Incident Response diensten op vergelijkbare wijze zijn ingericht, vaak volgens gangbare faseringen zoals triage, analyse, containment, herstel en evaluatie (bijv. gebaseerd op NIST). Daarnaast blijkt dat Incident Response zelden een geïsoleerde dienst is: de meeste partijen leveren deze in samenhang met andere diensten zoals: Digital Forensics, Threat Intelligence, Crisismanagement en communicatie, Security Operations (SOC), Consultancy en compliance, Business Continuity Planning (BCP). Ook is sprake van een modulaire opzet, waarbij afzonderlijke diensten afneembaar zijn, maar toch in een geïntegreerde aanpak worden geleverd. Er is ook sprake van duidelijke dwarsverbanden tussen technische, organisatorische en communicatieve disciplines, vaak georganiseerd rond een centraal incident response-team dat samenwerkt met andere expertgroepen. Een aantal partijen wijst erop dat de geschetste indeling sterk technisch is ingestoken en pleit voor een bredere benadering, waarin ook crisismanagement, reputatiebescherming en herstel (business recovery) structureel worden meegenomen.

Ad b. - Vrijwel alle marktpartijen benadrukken het belang van duidelijke rolverdeling en verantwoordelijkheden in het contract:

- Heldere taakafbakening: Wat doet de leverancier, wat blijft de verantwoordelijkheid van de deelnemer?
- Escalatieprocedures en contactpersonen: Wie mag opschalen en hoe is 24/7 bereikbaarheid geregeld?
- Toegang tot systemen en logdata: Vóóraf organiseren om vertraging te voorkomen.
- Forensische borging: Bewijslast en chain of custody volgens juridische eisen.
- Samenwerking met derden: Duidelijke afspraken over samenwerking met o.a. NCSC, interne SOC's, andere leveranciers.
- Rapportages en communicatie: Vaste formats, frequente updates, managementsamenvattingen.
- Oefeningen en evaluaties: Structureel leren van eerdere incidenten en paraatheid testen via tabletop-exercises.
- Contractvormen: Veel partijen werken met een retainer-constructie, waarbij bereikbaarheid, responstijden en scope vooraf zijn vastgelegd.
- Gebruik van tooling en automatisering: Verschillende partijen bieden automatisering van processen zoals triage, playbook-activatie, rapportage en integratie met ITSM-systemen.
- Er is brede consensus dat goede afspraken in de "koude fase" (voorafgaand aan incidenten) cruciaal zijn om effectief te kunnen reageren in de "warme fase".

Aandachtspunten en opvallende zaken

- Brede scope is belangrijker dan alleen technische IR - Meerdere partijen benadrukken dat effectieve incident response niet alleen een technische operatie is, maar ook organisatorische aspecten moet dekken, zoals crisismanagement, communicatie, business recovery en reputatieschadebeperking. Deze multidisciplinaire benadering wordt als essentieel gezien voor succesvolle incidentafhandeling.
- Verschillen in contractuele invulling en afhankelijkheden - Er is variatie in de wijze waarop partijen contracten aanbieden:
    - Sommige werken uitsluitend met een vooraf opgesteld retainer response plan.

  - Anderen bieden ook ondersteuning zonder retainer, maar wijzen erop dat dit leidt tot vertraging en hogere kosten.
  - Enkele partijen leveren IR alleen als onderdeel van een breder SOC-contract en ontraden standalone IR.
- Automatisering en integratie - Een groeiend aantal marktpartijen integreert automatisering in hun dienstverlening, zoals:
  - Automatische activatie van incident playbooks
  - Real-time dashboards
  - Koppelingen met detectieplatformen of ITSM-tools

  Deze aanpak verhoogt de snelheid en schaalbaarheid, maar vereist wel een zekere mate van volwassenheid aan klantzijde.
- Internationale inzet en schaalbaarheid **-** Sommige partijen benadrukken dat zij bij grootschalige of complexe incidenten kunnen opschalen via (inter)nationale netwerken of technologiepartners. Dit biedt flexibiliteit, maar stelt ook eisen aan de afspraken over bevoegdheden en samenwerking.
- Behoefte aan onboarding en voorbereiding - Verschillende partijen benoemen expliciet het belang van onboarding, inclusief het leren kennen van het IT-landschap, betrokken belanghebbenden en procedures van de deelnemer. Een goed georganiseerde onboarding vergroot de effectiviteit van de respons significant.

IR2 – [95%] Moeten we (en zo ja: hoe?) prijstechnisch rekening houden in het onderscheid in prijsmodel en prijsstelling van zaken die met of zonder spoed (Golden Hour) moeten worden opgepakt?

a. Als dat onderscheid er is: welke typen zijn daarin en hoe kan hiermee effectief/efficiënt worden omgegaan?
b. Is er een generieke kwalificatie waarin u breed in de markt niveaus van dienstverlening herkent? (e.g. Gold/Silver/Bronze, anders…)
c. Welke classificaties van reactie-/responstijden of andere 'levertijden' zijn bepalend voor het kunnen leveren van de diensten en wat is het effect van deze classificatie op de prijsstelling? Maak eventueel onderscheid naar verschillende diensten en geeft eventuele randvoorwaarden aan in de samenwerking met een Deelnemer.

Vrijwel alle marktpartijen geven aan dat het onderscheid tussen spoed (Golden Hour) en niet-spoed cruciaal is voor een passende prijsstelling, dienstverlening en SLA-afspraken. Dit onderscheid vertaalt zich in verschillende prijsmodellen (zoals spoedtarieven, retainers, toeslagen) en dienstverleningsniveaus (Gold/Silver/Bronze of vergelijkbaar).
Een breed gedragen reactie is dat een duidelijk classificatiemodel dienstniveaus en prijsstelling transparant en voorspelbaar maakt. Opvallend is dat enkele partijen maken bewust géén prijsverschil tussen Gold/Silver/Bronze en de classificatie enkel gebruiken om het aantal vooraf afgesproken uren te duiden. Deze partijen hanteren standaard uurtarieven die afhankelijk zijn van het moment op de dag (kantooruren, avond, nacht) dat de inzet wordt gevraagd.

Ad a. - Onderscheid in typen en prijsmodellen

- Spoedinzet / Golden Hour:
  - Reactie binnen 1 uur (soms zelfs binnen 30 minuten).
  - 24/7 beschikbaarheid.

  - Vraagt stand-by capaciteit, directe mobilisatie en ervaren IR-specialisten.
  - Prijsmodel: hogere tarieven, toeslagen buiten kantooruren, of een retainer met stand-by vergoeding.
- Versnelde IR:
  - Reactie binnen 2–4 uur.
  - Vaak tijdens of net buiten kantooruren.
  - Iets lagere kosten dan Golden Hour.
- Reguliere / Geplande inzet:
  - Reactie binnen 24 uur of langer.
  - Wordt vooraf ingepland.
  - Kostenefficiënt; lagere uurtarieven, geen toeslagen of stand-by verplichtingen.

Randvoorwaarden voor een effectieve aanpak:
- Classificatie bij melding (automatisch of handmatig) om snel het juiste niveau toe te wijzen.
- Duidelijke afspraken vooraf over spoedcriteria en escalatieprotocollen.
- Gebruik van retainers om beschikbaarheid te garanderen zonder per inzet te factureren.
- Strippenkaart- of abonnementsmodellen voor voorspelbaarheid in kosten.
- Inzet van tooling en SOC-detectie voor vroege herkenning en automatische dispatching.

Ad b. - Breed herkend marktmodel
Veel marktpartijen gebruiken of herkennen een gelaagd model, meestal:
- GOLD / PLATINUM:
  - 24/7 beschikbaarheid.
  - Reactie binnen 1 uur.
  - Toegang tot senior specialisten.
  - Inclusief tooling, monitoring en SLA-garanties.
- SILVER:
  - Beperkte beschikbaarheid buiten kantooruren.
  - Reactietijd binnen 4 uur.
  - Basisautomatisering en monitoring.
- BRONZE:
  - Alleen inzet tijdens kantooruren.
  - Reactie binnen 24 uur of best-effort.
  - Geen 24/7 dekking, lagere SLA-verplichtingen.

<u>Alternatieve kwalificaties:</u>
Sommige partijen gebruiken geen kleurcodering, maar onderscheiden retainer-gebaseerde inzet vs. ad-hoc inzet, of onderscheiden tussen spoed (incident response) en advieswerkzaamheden.
Enkelen maken bewust géén prijsverschil in Gold/Silver/Bronze, maar worden deze niveaus enkel gebruikt om het aantal vooraf afgesproken uren te duiden.

Ad c. - Classificatie van responstijden (en prijseffecten):

Urgentieklasse	*Reactietijd*	*Prijseffect*

Golden Hour	Binnen 1 uur (soms 30 min)	Hoogste tarief; stand-byvergoeding; premium-uren
High Priority	Binnen 2–4 uur	Hogere kosten; mogelijk toeslag buiten kantooruren
Standaard / Planbaar	Binnen 8–24 uur	Standaard tarief, geen toeslagen

Randvoorwaarden voor dienstverlening:

- Toegang tot logging/systemen bij start incident response.
- Bereikbaarheid van sleutelpersonen bij de deelnemer.
- Heldere escalatieprocedures (liefst vooraf gedefinieerd).
- Definitie spoed vs. niet-spoed moet contractueel worden vastgelegd.
- Communicatiekanalen (telefoon, mail, Signal/Telegram) voor noodmeldingen.
- Goedgekeurde beslissers aan klantzijde voor activering spoedinzet.

Bijzonderheden en aanvullingen:

- Één partij ziet retainer vooral als inefficiënt; stelt voor alleen te factureren bij daadwerkelijke inzet (i.p.v. paraatheid vooraf).
- Één partij hanteert geen prijsverschil tussen retainer-uren en ad-hoc inzet, maar wel hogere prijsfactor bij nachtinzet.
- Één partij behandelt álle incidenten met gepaste spoed, zonder prijsdifferentiatie; gebruikt aanpasbare abonnementen met 'tiers'.

IR3 – [100%] Welk prijsmodel acht u het meest passend voor deze vormen van dienstverlening, dienstig aan te leveren kwaliteit en besteding van algemene middelen (belastinggeld).

Op hoofdlijnen worden er drie varianten aangeboden:

Retainer-model (ca 45%)	Er wordt een maandelijkse of jaarlijkse vaste vergoeding in rekening gebracht voor zowel de 24/7 beschikbaarheid. Bij het retianermodel zijn uren voor inzet bij incidentresponse ingebrepen. Sommige respondenten vullen dit aan uren op nacalculatie waardoor het ook enigszins het karakter van een hybride model krijgt.
Hybride model (ca 50%)	Een abbonementsvorm voor paraatheid en beschikbaarheid, echter uren voor inzet bij incidentresponse worden op basis van verloonde uren op nacalculatie verrekend.
Abonnement + tickets (ca 10%)	Deze vorm is nagenoeg identiek aan het hybride model, echter in plaats van verrekening op basis van verloonde uren voor incident-response vindt verrekening plaats op basis van verbruikte tickets.

Typische componenten vaste prijs:

- 24/7 beschikbaarheid

- Bereikbaarheid via hotline
- Onboarding & intake (SOW, procedures, playbooks)
- SLA-afspraken en paraatheid
- Technische voorbereiding (bijv. EDR-integratie)

Typische componenten variabele prijs/verrekening op nacalculatie:

- Uurtarieven op basis van functieniveau
- Opslag voor inzet buiten kantoortijden, weekend of nachten
- Aparte tarieven voor acute incidenten (Golden Hour) vs. planbare forensische taken
- Projectprijzen voor planbare diensten (bijv. trainingen, simulaties, assessments)

Bijzonderheden en aandachtspunten:

- Herbestemming ongebruikte uren: Uren die niet gebruikt worden voor incidentresponse voor andere doeleinden inzetten
- Incident-specific scoping: Opstellen van een Scope of Work (SOW) voorafgaand aan een groter inzet.
- Tiered modellen: Verschillende pakketten (bijv. Gold/Silver/Bronze of klein/middel/groot) op basis van behoefte.
- Afhankelijkheid van klantvolwassenheid: Hoe volwassen een organisatie is bepaald benodigde inzet.

IR4 – [100%] Om te bepalen hoeveel Opdrachtnemers bij een raamovereenkomst te kiezen, speelt de vraag hoeveel klanten een Opdrachtnemer 24x7 kan bewaken en hoeveel in 'real time' gelijktijdig bij incidenten kunnen worden ondersteund. In dat kader wordt gevraagd naar uw mogelijke ervaring of uw beelden bij dit vraagstuk, met name bij vragen als :

1. Zijn objectieve gegevens te bepalen die deze verhouding kunnen uitdrukken, zodanig dat deze over diverse opdrachtnemers als benchmark kunnen worden gelezen?
2. Hoe bepaalt u deze verhouding als beheersbaar?
3. Hoe beheert/ondervangt u ter zake risico's?

Ad 1. - De meeste marktpartijen geven aan dat er zeker objectieve parameters zijn die gebruikt kunnen worden om de verhouding tussen capaciteit en klantondersteuning in Incident Response (IR) weer te geven. Tegelijkertijd wordt breed erkend dat een eenduidige, universele benchmark lastig **is**, vanwege de grote verschillen in klantomgevingen, typen incidenten, serviceniveaus en volwassenheid van tooling en processen.

Veelgenoemde objectieve maatstaven zijn onder andere:

- Aantal IR-specialisten of FTE per klant, incident of type incident (bijv. 1 IR-specialist per 3–5 actieve incidenten).
- Responstijdstatistieken zoals:
  - Mean Time To Detect (MTTD)
  - Mean Time To Respond (MTTR)
  - Mean Time To Resolve (MTTRo)
- Capaciteitskengetallen zoals:
  - Klanten per analist
  - Incidenten per maand per klant
  - Bezettingsgraad van IR-teams

- Aantal assets onder bewaking

Verschillende partijen hanteren ook interne ratio's of capaciteitsmodellen, vaak gebaseerd op historische data, klantclassificatie of incidentzwaarte. Er is brede consensus dat benchmarks alleen zinvol zijn wanneer rekening wordt gehouden met factoren als klantvolwassenheid, type dienstverlening (stand-by vs. actief), SLA's en automatiseringsgraad.

Ad 2. - Capaciteitsplanning, schaalbaarheid en automatisering zijn cruciale instrumenten. Er zijn drie terugkerende pijlers:

1. Capaciteitsplanning en klantsegmentatie - De meerderheid plant capaciteit op basis van:
   - Incidenthistorie en risicoprofiel van klanten
   - SLA-verplichtingen (bijv. responstijd binnen 15 min. of 4 uur)
   - Verwachte piekbelasting of seizoensinvloeden
   - Scoping van klantomgevingen bij contractstart
2. Schaalbaarheid en flexibiliteit **-** Veel partijen hanteren een gelaagd model met:
   - Kernteams
   - Interne flexibele schil of standby-teams
   - Opschaling via internationale of partnernetwerken
3. Automatisering en tooling - Door toepassing van:
   - SIEM/SOAR-platforms
   - Playbooks
   - CTI-feeds
   - Real-time dashboarding wordt de operationele druk verlaagd, waardoor met minder mensen meer klanten bediend kunnen worden.

Daarnaast geven meerdere partijen aan dat de verhouding continu wordt gemonitord en bijgestuurd, mede op basis van lessons learned en performance-analyses.

Ad 3. - Marktpartijen nemen overwegend een gelaagd risicobeheermodel in gebruik, waarbij risico's rondom piekbelasting, gelijktijdige incidenten en resourcebeschikbaarheid worden gemitigeerd via:

1. Redundantie en fallback-capaciteit, zowel in personeel (intern/extern) als tooling.
2. Opschalingsprocedures en escalatieprotocollen, waaronder P1-protocollen en prioritering bij gelijktijdige incidenten.
3. Continue monitoring van bezetting, belasting en responstijden via tooling en dashboards.
4. Proactieve crisisvoorbereiding, o.a. via:
   - Breach & Attack Simulations (BAS)
   - CTI-monitoring van dreigingstrends
   - Regelmatige test- en evaluatiemomenten

Een aantal partijen benadrukt het belang van samenwerking met meerdere opdrachtnemers of het hanteren van een multivendorstrategie binnen raamovereenkomsten om afhankelijkheden te minimaliseren en de continuïteit te waarborgen.

Aandachtspunten en opvallende zaken:

- *Geen universele standaard, wel richtinggevende indicatoren* - Ondanks dat er geen uniforme benchmark bestaat, is er wél brede consensus over het gebruik van bepaalde kengetallen. Deze kunnen worden ingezet voor onderlinge vergelijking, mits context wordt meegewogen.

- *Gelaagde opschaling als norm* - Bijna alle marktpartijen hanteren een model met vaste kernteams, flexibele interne schillen en/of internationale of partnernetwerken voor opschaling.
- *Automatisering als onderscheidende factor* - Organisaties met geavanceerde automatisering (SOAR, playbooks, CTI-integratie) rapporteren een hogere mate van beheersbaarheid en responssnelheid, zelfs bij gelijktijdige incidenten.
- R*ijksbrede of bredere raamcontracten* - Enkele partijen suggereren expliciet dat het hanteren van meerdere opdrachtnemers in een raamovereenkomst — bij voorkeur met fallbackafspraken — zorgt voor meer flexibiliteit en robuustheid.
- *Incidentgolven moeilijk voorspelbaar* - Diverse partijen wijzen erop dat incidenten vaak in golven optreden (bijv. zero-days als Log4j) en daardoor moeilijk voorspelbaar zijn. In zulke gevallen is snelle herverdeling van capaciteit essentieel.
- *Meertaligheid & wereldwijde dekking* - Enkele grote partijen benoemen de noodzaak om taaleisen niet te strikt te hanteren, zodat internationale expertise beter benut kan worden in schaarste- of crisissituaties.

IR5 – [100%] Kunt u de geschetste dienstverlening voor operationele incident response (IR 3.4.1 a t/m c) uitvoeren ingeval een andere leverancier zorgdraagt voor monitoring en detectie? Welke specifieke aandachtspunten ziet u hierbij?

De meerderheid van respondenten geeft aan dat ze onder voorwaarden operationele incident response kunnen leveren indien monitoring en detectie is ondergebracht bij een andere leverancier (één respondent geeft deze mogelijkheid zonder het noemen van voorwaarden):

- *Communicatie en coördinatie*: Afspraken over communicatie en coördinatie, inclusief heldere escalatieprocedures
- *Taakverdeling*: Duidelijke taakverdeling en afbakening van verantwoordelijkheden.
- *Informatie-uitwisseling*: Volledige en veilige overdracht van incidentinformatie; overeenstemming over classificering, prioritering en context; gedeeld incidentenregister;
- *Toegang tot logdata en systemen*: Toegang tot relevante logdata, detectie-informatie; toegang tot het SIEM systeem.
- *Duidelijke afspraken en contractueel borgen*: Juridisch/operationele afspraken en verplichtingen die de SOC-dienstverlener heeft, bijvoorbeeld 24/7 samenwerking, moeten contractueel zijn vastgelegd.

Aanvullend:

- Een First Incident Readiness Assessment is vooraf nodig;
- Integratie van tooling [tussen verschillende partijen];
- Het combineren van Incident Response met SOC-dienstverlening kan efficiënter (goedkoper) zijn.

Twee partijen geven aan niet bereid of in staat te zijn Incident Response uit te voeren wanneer monitoring & detectie elders is belegd.

IR6 - [45%] Hieronder is ruimte voor uw eventuele aanvullende reactie.

- *Incident Response is meer dan techniek* - Respondenten benadrukken dat IR niet alleen technisch moet worden ingericht, maar een organisatiebreed vraagstuk is. De juridische,

organisatorische en bestuurlijk inrichting moet goed moet worden geborgd. Ook de organisatorische rolverdeling en het belang van duidelijkheid in wie de regie voert bij incidenten is van belang voor adequaat incident response.

- *Voorbereiding is cruciaal* ("IR readiness") - Veel partijen vinden de aandacht voor voorbereiding, oefenen en leren te beperkt in de huidige opzet. Ze vragen expliciet om structurele borging hiervan. Meer concreet zijn de volgende onderdelen genoemd:
    - Meer nadruk op het op orde hebben van processen en forensische voorbereiding; Mogelijkheid van een forensisch readiness assessment.
    - Meer aandacht voor crisisvoorbereiding (plannen, oefenen), zoals door NCSC aanbevolen.
    - Overweeg verplichte post-mortem analyses voor ernstige incidenten en het koppelen van IR aan BAS en threat intelligence.
- *Kostenmodellen en paraatheid* - Eén partij geeft een visie op prijsmodellen en schaalbaarheid, wat relevant is voor kosteneffectiviteit en contractvorming. Genoemd worden:
    - Prijsstelling urgent vs. niet-urgent
    - Stand-by modellen voor "golden hour"-incidenten
    - Hybride prijsmodellen voor balans tussen kosten en paraatheid
- *Geïntegreerde benadering* - Meerdere respondenten pleiten voor het integreren van IR met bredere cybersecuritymaatregelen, inclusief toekomstige dreigingen. Meer specifiek wordt genoemd:
    - Integratie van IR met andere diensten zoals cryptoregistratie en threat intelligence (zeker m.b.t. post-quantum security).
    - Synergievoordelen als SOC en IR bij dezelfde partij zijn ondergebracht.
- *Ervaring en expertise als criterium* - Selectiecriteria zouden meer kunnen sturen op real-world ervaring en actuele dreigingskennis. Geef prioriteit aan partijen met aantoonbare praktijkervaring, vooral bij natiestaatdreigingen.
- *Data-autonomie en compliance* - Verwijzing naar actuele maatschappelijke en geopolitieke zorgen rond datatoegang en governance, echter zonder concrete voorstellen op welke wijze dit voor deze dienst relevant is.

3.4.2 (Cyber) Threat Intelligence

TI1 – [90%] Is bovenstaande opsomming dekkend voor de type TI-dienstverlening of zijn er varianten die hierboven niet zijn benoemd, maar wel in het kader van de beoogde raamovereenkomsten relevant zijn?

Over het algemeen wordt de opsomming als grotendeels dekkend ervaren. De TI-diensten zoals benoemd worden breed herkend, maar in de praktijk is ook behoefte aan uitbreiding met specialistische of niche-varianten, zoals sectorspecifieke threat intelligence, geopolitieke analyses, of maatwerkonderzoek naar dreigingsactoren.
Leveranciers van TI kunnen gespecialiseerd zijn in de verschillende soorten collectie, OSINT, SOCMINT, HUMINT of anderszins. Het is zinvol per use-case te bekijken welke type collectie(s) het beste past. Ook het doel (beleid, forecast, reageren op eventualiteiten) en niveau (strategisch, tactisch, operationeel) van gevraagde TI kan een verschil maken in wat

nodig is aan verrijken, contextualiseren en actualiseren van informatie. Belangrijk is een heldere eenduidige definitie c.q. afbakening.
Sommigen zien overlap met onder andere TI bij SOC-diensten en vinden bepaalde type TI daaraan gekoppeld zinvoller dan als aparte dienstverlening gecontracteerd, daar waar voor Red Teaming het juist reden kan zijn dit wel separaat te betrekken.

TI2 – [100%] Wat is naar uw beeld de beste strategie van het plaatsen van TI-dienstverlening en scopeafbakening? Als apart aan te besteden raamovereenkomst of als onderdeel van een ander RVICTO-onderdeel? Zie in dit licht ook onderstaande vragen met betrekking tot zinvolle clustering of separatie van diensten.

Een meerderheid geeft aan dat dreigingsinformatie het beste apart kan worden aanbesteed, gezien de specifieke expertise, marktwerking en onafhankelijkheid. Dreigingsinformatie vergt gespecialiseerde tooling en kennis. Separaat aanbesteden vergroot de kans op deelname van nichepartijen met die gespecialiseerde tooling en kennis.
Enkele respondenten zien niettemin bepaalde dreigingsinformatie als logisch te combineren met SOC-diensten, Incident Response en Forensisch Onderzoek, vanwege de inhoudelijke samenhang. Bundeling kan dan leiden tot synergie en snellere incidentafhandeling.
Ook is sprake van dreigingsinformatie-activiteiten van partijen die deze niet als datafeed of anderszins aan klanten leveren, maar gebruiken om de eigen MXDR-diensten te voeden.

TI3 – [90%] Ziet u de genoemde TI-diensten als logische verzameling die elke TI-dienstverlener standaard kan bieden, of betreffen het (ook) specifieke en dusdanig afwijkende diensten die door verschillende (gespecialiseerde) partijen wordt geleverd?

Overwegend wordt geoordeeld dat marktpartijen mogelijk (al dan niet in samenwerking met anderen) de TI-diensten kunnen leveren, zij het niet alles standaard door elke aanbieder zelf. De TI-markt is gegeven de diversiteit in de materie gefragmenteerd. Meerdere respondenten benadrukken dat sommige onderdelen (zoals datafeeds, dreigingsbeelden of diepgaande actor-analyses) alleen door gespecialiseerde partijen geleverd kunnen worden. TI omvat zowel standaarddiensten (feeds, baseline dreigingsinformatie) als specialistische producten (maatwerkonderzoek), waardoor differentiatie in aanbesteding belangrijk is. Ook is genoemd dat de informatie en bronnen in combinatie met de analist c.q. de menselijke factor het verschil maakt: het succes van dreigingsinformatie ligt niet sec in de dreigingsinformatie zelf.

TI4 – [50%]Hieronder is ruimte voor uw eventuele aanvullende reactie.

Dreigingsinformatie is een specialistisch domein en vraagt heldere scope en kwaliteitskaders. Duidelijke kwaliteitscriteria, borging van integriteit van data, en aandacht voor samenwerking met nationale bronnen (zoals NCSC) zijn essentieel. Ook wordt het advies voor separate dienstverlening herhaald, als ook het belang van kennis van de klantorganisatie als succesvoorwaarde en het afstemmen van de dreigingsinformatie hierop.

3.4.2-a. Datafeed ten behoeve van een SOC

DF1 – [100%] Welke CTI-datafeeds voor een SOC onderscheidt u en kunt u leveren? Beschrijf hierbij kort waar deze feeds in voorzien, hoe de data is verzameld (bronnen) en de integriteit (betrouwbaarheid, juistheid, volledigheid) is geborgd.

Hoewel niet alle partijen datafeeds leveren, is er desondanks brede beschikbaarheid van dreigingsinformatie, variërend van ruwe IOC-data tot verrijkte analyses**.** De meeste respondenten geven aan diverse soorten informatie te kunnen leveren, vaak onderverdeeld in *technische feeds* (IOC's, malware-signaturen, domeinen/IP's), *tactische feeds* (dreigingsactoren, campagnes) en *strategische feeds* (trends, sectoranalyses). Vaak genoemd zijn zowel *open source*, *commerciële feeds* als *eigen verzamelde informatie* (bijv. via SOC's en internationale samenwerkingen). Men werkt ook met/via platforms waarop datafeeds van klanten of derden kunnen worden aangesloten. Het gebruik van validatiemechanismen (menselijke factor) wordt benadrukt, als ook correleren met meerdere bronnen en filtering om betrouwbaarheid en volledigheid te waarborgen.
Niet iedereen ziet een datafeed als zinvol op zichzelf staand product, omdat de kwaliteit zonder nadere bewerking van beperkte waarde is en de kosten om dit naar de beoogde kwaliteit te brengen niet commercieel goed haalbaar is (mede in relatie met de gepercipieerde afnemersmarkt). Daarnaast is (bulk)doorlevering van datafeeds vaak niet toegestaan of vergt dat specifieke (kostbare) contractuele afspraken.

DF2 – [90%] Welke randvoorwaarden stelt u aan de Deelnemers bij het eventuele gebruik van deze CTI-datafeeds? Welke aandachtspunten of adviezen wilt u deze Deelnemers meegeven?

Niet iedere datafeed vanuit de klant is zonder meer aan te sluiten op een SOC-dienst. Dit vergt een goede integratie met bestaande SOC/SIEM-tools; duidelijke (juridische) afspraken over licentie, eigendom (met name t.a.v. profielen op de ruwe data) en vertrouwelijkheid (waaronder ook privacygevoelige data). Meerdere respondenten adviseren vooraf te zorgen voor afstemming met het SOC over formaten, technische koppelingen (API's) en classificatie van data. Ook klinkt een waarschuwing voor kwantiteit boven kwaliteit: meer indicatoren zonder context levert niet altijd meerwaarde en is mogelijk zelfs contraproductief qua inzet en focus.

DF3 – [90%] Welk prijsmodel hanteert u bij deze CTI-datafeeds? Wat zijn belangrijke kostendrivers (factoren die de hoogte van de prijs voor de Deelnemer bepalen)?

Het meest genoemd zijn abonnementsmodellen (per feed of per pakket), soms aangevuld met pay-per-use of volumebased modellen. De hoogte van de kosten worden beïnvloed door onder andere het aantal en (algemene/specifieke) type feeds, de mate van verrijking/analyse, licentievoorwaarden, integratiekosten en de schaal (aantal gebruikers of aangesloten systemen), waarbij strategische of verrijkte feeds vaak een hogere prijs hebben dan ruwe IOC-data.

DF4 – [50%] Hieronder is ruimte voor eventuele aanvullende reactie.

Er is noodzaak van internationale samenwerking, standaardisatie van formaten en het vermijden van overlap met bestaande nationale initiatieven (zoals NCSC-feeds). Ook is de rol van AI met betrekking tot dreigingsinformatie genoemd. In het algemeen wordt vooral het belang van kwaliteit en bruikbaarheid van feeds, en de rol van afstemming met bestaande ecosystemen bevestigd.

3.4.2-b. Dreigingsbeeld voor een Pentest

DP1 – [80%] Hier is geen vraag. U kunt onverminderd onderstaand desgewenst uw eventuele reactie geven.
Men kent dreigingsbeelden als voorbereiding op Pentesten, maar ziet het ook snel als 'overkill' voor een Pentest. Men werkt meer met een meer specifieke en gerichte voorbereidingen per pentest. Meer algemene periodieke dreigingsbeelden op organisatieniveau kunnen daarbij een aanvullende rol spelen. Daar waar een Pentest richting een Red Teaming opschuift, zullen ook de beoogde dreigingsbeelden vergelijkbaar mee schuiven.

3.4.2-c. Dreigingsbeeld voor Red Teaming

DR1 – [100%] De voornoemde Praktische Inkooprichtlijnen voor Red-teaming testen verwijzen naar kwaliteitseigenschappen van zowel de TI-provider, de TI-manager en het TI-team. Dit gelezen hebbende: welke minimumeisen (ja/nee) en subgunningscriteria kunnen naar uw mening het beste worden ingezet in de keuze van een partner voor de raamovereenkomst en wat resteert daarna aan onderscheidend vermogen voor gunning van een Nadere overeenkomst?
In het algemeen komt het neer op harde eisen voor basisniveau, met daarop ruimte voor differentiatie via kwaliteit en ervaring. Meerdere respondenten noemen als minimale vereisten verplichte certificeringen (o.a. CREST, TIBER-EU, ISO 27001) en (vooral) aantoonbare ervaring met complexe red teaming-projecten, als ook het gebruik van erkende frameworks. Voor analisten die een dreigingsbeoordeling doen is twee jaar relevante werkervaring wel het minimum. Mogelijk onderscheidend vermogen ligt onder andere in de kwaliteit van dreigingsanalyse gericht op de betreffende omgeving en organisatie, de mate van realisme in scenario's, flexibiliteit in aanpak en kwaliteit van rapportage. Het verschil wordt gemaakt veelal met name gemaakt in de diepgang van de analyse, toegang tot informatiebronnen, creativiteit in scenario's en de ervaring van het team. NB: niet alle partijen die Red Teaming doen leveren ook losse TI-scenario's.
DR2 – [90%] Welke vormen van dreigingsbeelden voor Red Teaming test onderscheidt u en kunt u leveren? Beschrijf hierbij kort waar deze dreigingsbeelden in voorzien, hoe de data is verzameld (bronnen), de beelden tot stand komen (analyse) en de integriteit (betrouwbaarheid, juistheid, volledigheid) is geborgd.
De meeste respondenten onderscheiden operationele, tactische en strategische dreigingsbeelden/scenario's voor realistische aanvalssimulaties, gebaseerd op actuele dreigingsactoren, aanvalstechnieken en sectorgerichte risico's. Hiervoor gebruik men een mix van bronnen: open source, commerciële feeds, interne data uit SOC's en uit de samenwerking met NCSC en sectororganisaties. De integriteit van de scenario's wordt geborgd door validatie via meerdere bronnen, peer review en gestructureerde analysemethoden. De RT-dreigingsbeelden zijn divers en modulair inzetbaar. De betrouwbaarheid ervan is een cruciale succesfactor.

DR3 – [90%] Welke randvoorwaarden stelt u aan de Deelnemers en de Red Teaming Provider (RTP) bij de aanvraag en het gebruik van deze dreigingsbeelden? Welke aandachtspunten of adviezen wilt u meegeven?
Randvoorwaarden komen vooral vanuit de regelgevende instanties en opdrachtgever. Dreigingsbeelden/scenario's voor Red Teaming moeten maatwerk zijn en afgestemd op de organisatiecontext. Voor het succesvol kunnen voldoen aan verwachtingen rond de uitvoering van een opdracht is het zaak vooraf duidelijke scopeafspraken te maken, het beschermen van vertrouwelijke data een voorwaarde, als ook een goede communicatie tussen Red Team, opdrachtgever en eventuele derde partijen. Ook is het zaak kenbare risicomanagement te hebben op mogelijke misinterpretatie of onvoldoende actualiteit met periodieke updates en toetsing van de bestaande beelden. De randvoorwaarden liggen vooral op governance, afstemming en borging van actualiteit en vertrouwelijkheid.
DR4 – [90%] Welk prijsmodel hanteert u bij deze dreigingsbeelden voor Red Teaming? Wat zijn belangrijke kostendrivers (factoren die de hoogte van de prijs voor de Deelnemer bepalen)?
Het meest genoemd zijn vaste prijs per dreigingsbeeld. De hoogte wordt bepaald door onder andere de complexiteit van de analyse, benodigde bronnen (open/commercieel), mate van maatwerk, en frequentie van updates. Op de vaste prijs is ook een flexibele verrekening van meerwerk genoemd voor verdieping of uitbreiding van de scope. Sommigen hanteren een modulair prijsmodel. Een prijs is sterk afhankelijk van gewenste/benodigde diepgang en frequentie.
DR5 – [10%] Hieronder is ruimte voor uw eventuele aanvullende reactie.
Hier is een reactie gegeven op overwegingen om zowel RT als TI opdragen aan één partij, dan wel RT en TI separaat aan verschillende partijen opdragen. Voor beide varianten valt wat te zeggen.

3.4.2-d. Generieke/specifieke dreigingsbeelden

DB1 – [100%] Heeft u in uw dienstportfolio van informatiediensten het genereren en onderhouden van generieke en (organisatie-) specifieke dreigingsbeelden? Zo ja: a) Hoe kunnen die onderscheidenlijk als in de markt breed herkenbare c.q. erkende af te nemen producten worden getypeerd/omschreven? b) Is het beroep op die informatiedienst periodiek, ad hoc? c) Zijn er aanpalende (advies-)diensten verbonden, maar separaat van de informatiediensten? d) Is er een zinvolle clustering of separatie van informatiedienst zoals u die heeft omschreven en waarom?
Het wordt niet overal evenzeer als bestaande vraag uit de markt herkend, maar een meerderheid van de respondenten bevestigt dat zij zowel generieke als organisatie-specifieke dreigingsbeelden aanbieden, zowel periodiek als ad hoc: • Generiek: breed toepasbare producten zoals sectorrapporten, baseline dreigingsbeelden, jaarlijkse analyses.

- Specifiek: maatwerkrapportages gericht op de eigen organisatie, vaak ad hoc of periodiek geüpdatet.

Dreigingsbeelden worden vaak gecombineerd met advies of consultancy (bijvoorbeeld risicobeoordeling, compliance-advies, strategische securityplannen). Veel respondenten zien waarde in een separate opdracht, zodat generieke en specifieke beelden onafhankelijk afneembaar zijn. Ook speelt hierin een rol dat veel generieke beelden sowieso periodiek worden gepubliceerd. De behoefte is vormt zich mede op basis van wat er aan behoefte is bovenop reeds gepubliceerde informatie.

DB2 – [80%] Welk prijsmodel acht u het meest passend voor deze dienstverlening dienstig aan te leveren kwaliteit en besteding van algemene middelen (belastinggeld).

De meeste respondenten noemen (voor zover niet al openbaar toegankelijk) abonnement-modellen voor generieke beelden (vast bedrag per periode) en maatwerkoffertes met vaste prijs of uurtarieven voor specifieke beelden. Dit kan zit ook uiten in een basisabonnement met aanvullende modules of maatwerkproducten. Bij maatwerk zijn kostenbepalende factoren: diepgang van de analyse, mate van maatwerk, gebruikte bronnen (open/commercieel) en een eventuele updatefrequentie.

DB3 – [10%] Hieronder is ruimte voor uw eventuele aanvullende reactie.

Dreigingsbeelden, al dan niet specifiek verrijkt, zijn veelal opgenomen in een breder strategisch instrument en/of dienstverlening (RT, SOC, …). Qua relevante inhoud en insteek worden ze toegespitst op de beoogde doelgroep, van C-niveau tot techniek.

3.4.2-e. TI-onderzoeken

TO1 – [100%] Heeft u in uw dienstportfolio van informatiediensten TI-onderzoeken? Zo ja:
a) Hoe kunnen verschillende TI-onderzoeken onderscheidenlijk als in de markt breed herkenbare c.q. erkende af te nemen producten worden getypeerd/omschreven?
b) Is het beroep op die informatiedienst periodiek, ad hoc?
c) Zijn er aanpalende (advies-)diensten verbonden, maar separaat van de TI-onderzoeken?
d) Is er een zinvolle clustering of separatie van informatiedienst zoals u die heeft omschreven en waarom? Indien relevant kunt u ook de relatie leggen met hieronder 3.3.2-d.

TI-onderzoeken zijn zowel als standaardproducten als maatwerk beschikbaar, met sterke variatie in scope en toepassing. De meeste respondenten bevestigen TI-onderzoeken in hun dienstenpakket te hebben.

- Breed herkenbaar: actorprofilering, campagne-analyse, dark web monitoring, sectorgerichte onderzoeken.
- Specifiek/maatwerk: onderzoeken naar incidenten, supply chain dreigingen of geopolitieke risico's.

TI-onderzoeken worden vaak ad hoc (bij incidenten of specifieke vragen) verzocht, maar soms ook periodiek (bijv. kwartaalrapportages of terugkerende assessments).
Aan TI-onderzoeken zijn vaak adviesdiensten gekoppeld (zoals beleidsadvies, compliance-begeleiding of security-roadmaps), dan wel is het onderdeel van bredere dienstverlening.

Als TI-onderzoeken verbondenheid heeft met andere dienstverlening is het handiger het in dat verband mee te nemen in een opdracht. Dit laat onverlet dat het een specialistisch domein is dat goed separaat kan worden aanbesteed.
TO2 – [80%] Welk prijsmodel acht u het meest passend voor deze dienstverlening dienstig aan te leveren kwaliteit en besteding van algemene middelen (belastinggeld).
Het meest genoemd zijn projectprijzen of uurtarieven voor ad hoc onderzoeken, en abonnementen voor periodieke rapportages, waarbij ook een vaste basisprijs voor standaard TI-onderzoeken mogelijk is met aanvulling van maatwerkcomponenten. De prijs voor het maatwerk wordt bepaald door de complexiteit van het onderzoek, de benodigde bronnen (open vs. commercieel), gevraagde diepgang van analyse, en (niet in de laatste plaats) de urgentie. Met transparantie, flexibiliteit en voorspelbaarheid rond de kosten en het beprijzen kan kostenefficiënt met belastinggeld worden omgegaan.
TO3 – [20%] Hieronder is ruimte voor uw eventuele aanvullende reactie.
TI-onderzoeken zijn veelal opgenomen in een breder strategisch instrument en/of dienstverlening (onderbouwing dreigingsbeelden en voeden van simulatiescenario's). Diverse TI-producten, waaronder IT-onderzoeken, overlappen met andere TI-producten. Een goede analyse van de behoefte is geboden om een verstandige keuze in te betrekken TI-producten te maken.

3.4.3 (Social) Awareness

SA1 – [100%] In hoeverre onderscheiden type awareness-activiteiten rond informatieveiligheid en doelgroepen zich zodanig dat een bepaalde omvang clustering of separatie van awareness-activiteiten aan te raden is c.q. goed aansluit op de markt?
De meeste respondenten vinden dat awareness-activiteiten sterk verschillen per doelgroep en methode. Qua methoden onderscheiden zich op hoofdlijnen de actieve (groeps-)vormen (trainingen et cetera) van het aan bieden van awareness platforms, waar klanten zelf de eigen activiteiten kunnen doen. Doelgroepen kenmerken zich door hun rol ten opzichte van informatiebeveiliging en het gewenste niveau van awareness. Clustering van awareness-diensten in één geheel kan voordelen opleveren voor vergelijkbare behoeften (o.a. eindgebruikers), daar waar diverse behoeften (o.a. verdieping) wellicht beter af zijn met meer specifiek gerichte contracten (o.a. technici). Bij clustering moet worden gewaakt dat geen kwaliteitsverlies optreedt, omdat de markt gefragmenteerd is met veel specialistische aanbieders. Clustering en separatie zijn beiden relevant strategieën en niet een basis strategie voor het geheel van Awareness.
SA2 – [100%] Hoe en in hoeverre kunnen door u gebruikte manieren/methoden en/of de door u hierbij in te zetten expertise en/of in te zette hulpmiddelen bijdragen aan het onderscheidend vermogen tussen aanbieders?
Onderscheid wordt gemaakt in gebruikte methoden (e-learning, phishing-simulaties, gedragsprogramma's), in de kwaliteit van trainers/experts, en in de tooling en platforms die worden ingezet. Men heeft diverse focuspunten: compliance; gedrag en verandering;

termijneffect; programmatische benadering, …. Ook maatwerk, sectorspecifieke expertise en de combinatie van meten–trainen–testen worden genoemd als belangrijke onderscheidende factoren.

SA3 – [100%] Zijn er anders dan manieren/methoden, elementen waarop het succes van uw activiteiten zichtbaar gemaakt kan worden? Bij voorkeur zodanig dat daarmee ook vergelijking tussen marktpartijen mogelijk is.

Vaak genoemd worden KPI's zoals aantal afgeronde trainingen, klikratio's bij phishingtests en gedragsveranderingen. Niettemin geven meerdere respondenten geven aan dat standaardisatie (t.b.v. vergelijking) lastig is. Benchmarks zijn wel enigszins mogelijk via gestandaardiseerde formats en rapportages. Het lastige blijft hierbij wel, dat succes zich met name in minder goed direct meetbare aspecten laat zien, zoals cultuurverandering en bewustzijnsgroei. Toch kunnen meetbare aspecten bijdragen aan het onderscheidend vermogen, zoals de mate van deelname en resultaten door deelnemers, incidentreductie, feedback vanuit andere activiteiten, zoals bijvoorbeeld pentesten. Een ander onderscheidend element kan de klanttevredenheid van voorgaande opdrachtgevers zijn (referenties). Ook kan met vooraf een awareness meetbare doelen stellen waarop de effectiviteit kan worden gevolgd.

SA4 – [90%] Welke eisen zouden wij op het niveau van een raamovereenkomst moet stellen (geldend voor alle hieronder te verstrekken opdrachten)?
Met welke wensen kunnen wij een zinvol onderscheid maken tussen de niveaus van dienstverlening van aanbieders?

Eisen rond kwaliteit en certificering van trainers, beveiliging en privacy van gebruikte platforms, en bewezen effectiviteit van methodieken. Qua wensen liggen mogelijkheden voor onderscheid in mate van maatwerk, innovatie en continuïteit in programma's. De basisvereisten moeten basiskwaliteit waarborgen. Het verdere onderscheid tussen dienstverleners zit dan in de voorgestelde aanpak, ervaring met overheid, gebruik van frameworks, maatwerk en innovatie. Diverse voorbeelden zijn genoemd.

SA5 – [90%] Welk prijsmodel acht u het meest passend voor deze dienstverlening dienstig aan te leveren kwaliteit en besteding van algemene middelen (belastinggeld) en hoe beïnvloedt dit de vorige vraag V1?

De meeste respondenten noemen abonnementsmodellen (bijv. per gebruiker of per jaar) voor standaard e-learning en training. Maatwerkactiviteiten (workshops, campagnes) worden vaak op projectbasis of via strippenkaarten afgerekend met een vaste prijs. De hoogte van de kosten wordt bepaald door het aantal deelnemers, de gewenste diepgang van de training, gebruikte platforms/tooling en overige maatwerkfactoren.

SA6 – [30%] Hieronder is ruimte voor uw eventuele aanvullende reactie.

Een effectieve aanpak varieert naar gelang de doelgroep en het gestelde doel. Ter zake bewustzijn creëren richt zich op gedragsverandering. Dat is minder gebaat bij een eenmalige actie of interventie. Een structurele aanpak biedt gedane investeringen beter rendement met het onderhouden van het bewustzijn en de daarbij toe te passen blijvende actualiteit. Dat vergt

investeringen van leverancierskant, maar ook actieve betrokkenheid van opdrachtgevers om de middelen in communicatie en stijl op de organisatie aan te laten sluiten.

3.4.4. (Digitaal) Forensisch Onderzoek

FO1 – [100%] Heeft u in uw dienstportfolio het uitvoeren van (digitaal) Forensisch Onderzoek? Zo ja: a) Hoe kunnen verschillende vormen van digitaal Forensische onderzoeken onderscheidenlijk als in de markt breed herkenbare c.q. erkende af te nemen diensten worden getypeerd/omschreven? Welke vormen levert u? b) Zijn er aanpalende (advies-)diensten verbonden, maar separaat van de Forensische onderzoeken?
De meeste respondenten bieden meerdere vormen van digitaal forensisch onderzoek aan, al dan niet in samenwerking met c.q. uit te voeren door gespecialiseerde en gecertificeerde partners. Er worden meerdere type onderzoeken onderscheiden (zoals onder andere incident response-gerelateerde forensics, e-discovery, fraude-gerelateerde onderzoeken, chain-of-custody analyses, en malware- of loganalyse). Onderzoeken kunnen ook worden aangevuld met juridische ondersteuning, compliance-begeleiding of rapportages voor gerechtelijke procedures. Bij diverse respondenten is forensisch onderzoek onderdeel van hun Incident Response dienstverlening.
FO2 – [100%] Hoe en in hoeverre kunnen door u gebruikte manieren/methoden van onderzoek en/of de door u hierbij in te zetten expertise en/of in te zetten hulpmiddelen bijdragen aan het onderscheidend vermogen tussen aanbieders?
Het onderscheid zit vooral in de combinatie van methodiek, certificering en praktijkervaring. Vaak genoemd zijn zelf ontwikkelde methodieken, gebruik van internationaal erkende standaarden en specifieke tooling, als ook onderscheid via certificeringen, ervaring met juridische procedures en multidisciplinaire teams/domein overschrijdend onderzoek (IT, recht, opsporing). Er zijn ook verschillen in tooling (commercieel vs. open source) en mate van automatisering (o.a. AI) met daarin het verschil tussen online (Cloud) en on premise onderzoek-omgevingen.
FO3 – [100%] Welke eisen zouden wij op het niveau van een raamovereenkomst moet stellen (geldend voor alle hieronder te verstrekken opdrachten)? Met welke wensen kunnen wij een zinvol onderscheid maken tussen de niveaus van dienstverlening van aanbieders?
Eisen rond ketenborging (chain of custody), beveiliging en vertrouwelijkheid, certificering van onderzoekers en inzet van forensisch bewezen methodieken. Onderscheid kan worden gemaakt op aspecten als: snelheid van oplevering, ervaring met specifieke sectoren, of kwaliteit van rapportage.
FO4 – [90%] Welke randvoorwaarden stelt u aan de Deelnemers bij de aanvraag en het gebruik van deze Forensische Onderzoeken? Welke aandachtspunten of adviezen wilt u meegeven?

Randvoorwaarden liggen vooral op governance, juridische borging en toegang tot relevante data. Van opdrachtgevers/Deelnemers is nodig: een duidelijke scope en opdrachtdefinitie, snelle toegang tot relevante systemen/data, en heldere afspraken over eigenaarschap en gebruik van bevindingen. Meerdere respondenten wijzen op het belang van nauwe samenwerking met juridische teams en het vooraf afstemmen van de inzet van tooling en methodieken.

FO5 – [100%] Welk prijsmodel hanteert u bij deze Forensische Onderzoeken? Wat zijn belangrijke kostendrivers (factoren die de hoogte van de prijs voor de Deelnemer bepalen)?

Het meest genoemd zijn uurtarieven en projectprijzen, soms met vooraf afgesproken pakketten voor standaardonderzoeken. De hoogte van de kosten worden bepaald door de complexiteit en omvang van het incident, benodigde expertise, mate van juridische betrokkenheid, hoeveelheid te analyseren data en snelheid van uitvoering. Maatwerk en incidentafhankelijkheid bepalen de prijs; voorspelbaarheid is beperkt; transparantie is essentieel.

FO6 - [15%] Hieronder is ruimte voor uw eventuele aanvullende reactie.

Enkele respondenten benadrukken het belang van samenwerking met opsporingsinstanties en de rol van internationale standaarden, als ook het advies het samen te brengen met Incident Response. Forensisch onderzoek is een sterk gereguleerd domein dat hoge eisen stelt aan kwaliteit en betrouwbaarheid.

3.4.5 IB-consultancy

IB1 – [85%] In hoeverre wordt bij u al rekening houden met AI en Quantum cryptografie en heeft u daar een visie op? Hoe zou u deze elementen in een marktbenadering (aanbesteding) zinvol ingebed zien?

Meerdere respondenten geven aan al rekening te houden met AI-toepassingen (zowel als bedreiging, als hulpmiddel) en de toekomstige impact van quantum computing op cryptografie. Met betrekking tot de inzet van AI gaat het vooral om detectie, analyse en automatisering van beveiligingsprocessen. Ook kan AI een rol spelen in IB-risico's zoals met deepfakes en geavanceerde aanvallen. Het belang van post-quantum cryptografie is evident en de noodzaak om tijdig te migreren naar ter zake standaarden, voor zover die er zijn. Diverse respondenten geven aan al met PQC bezig te zijn c.a. rekening te houden. IB-aanbestedingen/-contracten moeten rekening moeten houden met innovatie, flexibiliteit en dus ruimte voor periodieke herijking van technologieën.

IB2 – [15%] Hieronder is ruimte voor uw eventuele aanvullende reactie.

Men noemt het belang van samenwerking met kennisinstellingen, aandacht voor ethische aspecten van AI, en de noodzaak van meer publieke regie rond quantum readiness. Er is de noodzaak van innovatie en samenwerking om voorbereid te zijn op toekomstige dreigingen.

RVICTO 2026 – MARKTRAADPLEGING - VERSLAG