

Algemene Eisen:

Nr.	Omschrijving
E1	Vanaf start van de overeenkomst dient in overleg overgegaan te worden tot implementatie, echter binnen 3 weken na de door de aanbestedende dienst gewenste starttermijn. De kosten van de dienstverlening worden in rekening gebracht vanaf de ingebruikname.
E2	Vanaf de start van de implementatie dient de dienstverlening binnen 3 maanden operationeel te zijn, inclusief de inrichting van het SIEM, onboarding van assets/logbronnen en de SOC dienst. De aanbestedende dienst bepaalt de begin en eindtijd van de implementatie termijn.
E3	De inschrijver rapporteert tijdens de implementatie wekelijks over de voortgang van de implementatie in relatie tot de planning (conform Project Initiatie Document/Project Plan)
E4	Alle verwerking van persoonsgegevens vindt plaats binnen de Europese Economische Ruimte (EER). Dat wil onder andere zeggen dat alle personeel, apparatuur, gegevensopslag en netwerkverbindingen die voor de aanbestedende diensten worden gebruikt, zich binnen de EER bevinden.
E5	De te leveren dienst voldoet aan de Baseline Informatiebeveiliging Overheid. https://bio-overheid.nl

Commerciële eisen:

Nr.	Omschrijving
E6	Inschrijver is bij haar inschrijving uitgegaan van geldende prijzen voor de dienstverlening en/of levering. Niet genoemde kosten kunnen onder geen geval alsnog in rekening worden gebracht bij de aanbestedende dienst. Hetgeen door inschrijver wordt uitgewerkt in het kwalitatief gunningscriterium is in de opgegeven prijs van inschrijver inbegrepen.
E7	Inschrijver verklaart dat hij ermee akkoord gaat dat prijswijzigingen niet eerder van kracht zijn dan na schriftelijke goedkeuring door Aanbestedende dienst.
E8	Inschrijver sluit onderhoudsovereenkomst af voor de gebruikte software met een looptijd gelijk aan de contractduur.
E9	Binnen de onderhoudsovereenkomst vallen ook de updates van software, besturingssystemen en eventuele firmware, ongeacht de versie(s) en (nieuwe/extra) functionaliteiten.
E10	Garantie en ondersteuning voor benodigde hard- en software dienen voor de gehele contractperiode te zijn afgekocht bij de fabrikant.
E11	Bij opdrachtverlening zal, indien van toepassing, de eventuele verrekening plaats vinden op basis van de werkelijk gerealiseerde aantallen.

Eisen aan ondersteuning:

Nr.	Omschrijving
E12	Inschrijver levert en/of implementeert alle producten, diensten en functionaliteiten zoals beschreven in dit document conform dit Programma van Eisen. Ook wanneer technische componenten benodigd voor gespecificeerde dienstverlening niet expliciet genoemd wordt.

E13	Inschrijver is bereid en in staat om op verzoek van en in overleg met de aanbestedende dienst eens per kwartaal de volgende service level rapportages te overhandigen: • Verrichtte requests/aanvragen van de aanbestedende dienst en status • Aantallen events/alerts, meldingen aan de aanbestedende dienst en incidenten naar classificatie, zoals informational, low, medium, high, critical • Beschikbaarheid van diensten SOC en SIEM over de rapportageperiode • Evaluatie en aanbevelingen • Klachten en klachtafhandeling
E14	Inschrijver stelt een vast contactpersoon (en vervanger) aan voor alle communicatie tussen de aanbestedende dienst en Inschrijver gedurende de implementatie en uiteindelijke acceptatie. De contactpersoon rapporteert tevens aan aanbestedende dienst op regelmatige basis de voortgang van openstaande issues/verbeterpunten. De aanbestedende dienst stelt ook een vast contactpersoon (en vervanger) aan.
E15	Inschrijver stelt zich als tactisch en strategische partner voor de aanbestedende dienst op. Dit houdt in dat zij proactief acteert op wijzigingen/verbeteringen of andere zaken welke betrekking hebben op de aangeboden oplossing. De frequentie van dergelijk overleg en deze activiteiten moet minimaal 1 maal per jaar zijn, in het eerste contractjaar minimaal 1 maal per kwartaal.
E16	De mate en vorm van communicatie wordt vastgelegd in een OLA of SLA. Deze dient vanuit inschrijver opgeleverd te worden. Een concept/voorbeeld aanleveren als bijlage aan uw inschrijving is een vereiste (toevoegen als bijlage 8).
E17	De inschrijver voorziet de aanbestedende dienst van advies en ondersteuning over communicatie- en handelingsplannen bij inbreuken.
E18	Inschrijver dient bij gunning, als aanvulling op de geëiste OLA / SLA, gezamenlijk een DAP overeen te komen waarin minimaal de navolgende onderwerpen belegd zijn: • Strategische en tactisch advies • Authorisatiematrix • Contactpersonen en stakeholders • Melding van en advies over door het SOC vastgestelde beveiligingsissues • Een klachtenprocedure • Problem support (actief en reactief) • Escalatiemodel (opdrachtnemer en opdrachtgever)

Eisen aan de leverancier en de toeleveringsketen:

Nr.	Omschrijving
E19	Bij het verlopen van ISO27001 certificaten of TPM verklaringen levert de inschrijver uit eigen beweging binnen 3 maanden geldige certificaten en verklaringen op aan de aanbestedende dienst.

SOC dienstverlening eisen:	Omschrijving
E20	Het SOC voert een triage en analyse uit op alerts vanuit het SIEM en ontlast daarmee de aanbestedende dienst optimaal

E21	Het SOC isoleert assets/plaatst deze in quarantaine om een aanval of inbreuk te dwarsbomen en/of in te dammen. Na gunning wordt afgestemd: - Communicatie en beslisprotocol met bevoegdheden van de inschrijver - Werkwijze per assettype afhankelijk van de functionaliteit van EDR en de toewijzing van bevoegdheden aan de inschrijver. Het gaat daarbij om containment, zodra een inbreuk is gedetecteerd.
E22	Het SOC voert de gehele incident response uit in nauw contact met de aanbestedende dienst. Het gaat over de regie in het incident response proces in afstemming met management van de aanbestedende dienst voor besluitvorming en beheerders van de aanbestedende dienst die door het SOC geconsulteerd zullen worden en die acties uitvoeren waartoe zij wel en het SOC niet geautoriseerd is.
E23	Het SOC start de triage/analyse van hoge/kritieke alerts binnen 10 minuten.
E24	Het SOC contacteerd de aanbestedende dienst binnen 30 minuten over hoge/kritieke alerts incl. status.
E25	Binnen het SOC dient de volledige footprint zowel on-prem alsook cloud bewaakt te worden en is het een vereiste dat alle systemen/endpoints 24x7 uur gemonitord worden
E26	aanbestedende dienst eist een redundante oplossing, zodat de dienstverlening bijv. tijdens onderhoud of storingen volledig operationeel blijft.
E27	De inschrijver kijkt breder dan alleen haar eigen dienstverlening en geeft ook pro-actief verbetervoorstellen aan

SIEM oplossing dienstverleningseisen:	Omschrijving
E28	De inschrijver biedt het SIEM als dienst aan, inclusief levering van software, inrichting en beheer. Voor lokale log-collectie mag gebruik gemaakt worden van een (kale) virtuele machine op basis van VMware, die door de aanbestedende dienst ter beschikking wordt gesteld.
E29	Voor het SIEM worden toekomstbestendige mainstream producten uit de markt ingezet met minimaal maatwerk. Producten waarvan de leverancier end-of-life heeft aangekondigd of een productstrategie waarin SIEM niet meer centraal staat, voldoen niet aan deze eis.
E30	De beschikbaarheid van het SIEM is 99,9% per maand excl. beschikbaarheid van een eventueel gebruikte (kale) VM die door de aanbestedende dienst ter beschikking wordt gesteld en excl. met de aanbestedende dienst afgestemde onderhoudsvensters (max 1 uur/maand).
E31	Rekening wordt gehouden met alle aanvalstechnieken van bijv. Mitre Att&ck of NIST framework af, voor zover relevant voor de assets in scope en voor zover detectie middels SIEM mogelijk is.
E32	De loginformatie wordt 13 maanden bewaard. Daarna worden de log-gegevens (semi-)automatisch verwijderd.
E33	Deze bewaartermijn is op wens van de aanbestedende dienst aan te passen. Toelichting: De aanbestedende dienst wil de flexibiliteit hebben de bewaartermijn aan te passen, wanneer daar gedurende de contractperiode aanleiding toe is, bijvoorbeeld bij voortschrijdend inzicht. In dat geval zou de bewaartermijn bijvoorbeeld uitgebreid kunnen worden naar 18 of 24 maanden.
E34	Aan het einde van het contract worden de loggegevens in het SIEM in een gestandaardiseerd formaat, zoals bijvoorbeeld JSON of XML, overgedragen aan de aanbestedende dienst.
E35	De complete omgeving, dus alle applicaties en onderliggende infrastructuur van de opdrachtnemer zijn ingericht conform de verplichte standaarden van het Forum Standaardisatie: zie link. https://www.forumstandaardisatie.nl/openstandaarden/lijst/verplicht , daarnaast is de dienst gekoppeld met voldoende of ruim voldoende versleuteling tussen opdrachtnemer en opdrachtgever volgens deze standaarden.

E36	Network Detection and Response dienstverlening en Threat intelligence dienstverlening maken onderdeel uit van de SIEM dienstverlening (zowel operationeel alsook financieel).
E37	SIEM/SOC bewaakt zowel het externe verkeer als het interne verkeer.
E38	Een logregel die doorgestuurd wordt bevat in geen geval gegevens die naar volledige persoonsdata (volledige BRP informatie) kan leiden.
E39	Koppelingen/verbindingen tussen systemen en/of services (ook als deze op hetzelfde systeem draaien) worden door opdrachtnemer bij inschrijving inzichtelijk gemaakt in een protocol matrix, waarin de verkeerstromen zijn opgenomen. Deze matrix bestaat minimaal uit de volgende velden: • Source IPv(4/6) • Source Port • Destination IPv(4/6) • Destination Port • Layer 4 protocol (bijv. TCP/UDP/...) • Application protocol (bijv.: http/https/smtp/dns/...).
E40	De dienst en onderliggende ICT-componenten zijn altijd upto-date. Opdrachtnemer mag maximaal 1 stabiele patch aan het einde van de train (bijv 1.0.0.1) achterlopen, mits deze versie nog volledig wordt ondersteund door de betreffende leverancier van dat component en geen kwetsbaarheden of bugs bevat.

