BIJLAGE 8 PROGRAMMA VAN EISEN

SIEM / SOC DIENSTVERLENING

I N H O U D S O P G A V E Pagina

1. Dienstverlening

Senzer heeft het voornemen om een Overeenkomst af te sluiten voor de SIEM/SOC Dienstverlening om de continuïteit van de dienstverlening informatiebeveiliging te kunnen (blijven) waarborgen.

Opdrachtnemer biedt een SIEM/SOC-oplossing aan welke binnen de infrastructuur van Opdrachtgever of binnen de infrastructuur van Opdrachtnemer wordt/is geplaatst.

Daarnaast moet vanuit de Opdrachtnemer ten allen tijde een CERT-team beschikbaar zijn in geval van een calamiteit. Bij calamiteiten moet een volwaardig CERT-team op de locatie van Opdrachtgever aanwezig zijn binnen 12 uur na melding van de calamiteit.

Omschrijving van de use cases (zowel technische als business) en ontwikkeling hiervan tijdens de dienst moet te worden beschreven.

Opdrachtnemer biedt duidelijk gecontroleerd proces voor het doorvoeren van veranderingen en moet de mogelijkheid te hebben deze veranderingen te testen voordat ze in productie gaan.

De geboden oplossing moet voldoende robuust te zijn om het benodigde volume aan logdata en events voor het totaal van Instellingen de Opdrachtgever te kunnen afhandelen en daarin mee te kunnen op- en afschalen bij meer/minder gebruik van de dienst.

De gevraagde diensten moeten eenvoudig, maandelijks, op- en afgeschaald te kunnen worden.

De data binnen het geboden platform moet ook ingezet te kunnen worden voor andere doeleinden zoals IT-operations en Business Intelligence middels standaard API’s of anderszins.

Opdrachtnemer is verantwoordelijk voor levering, installatie, configuratie, beheer en onderhoud van de SIEM-oplossing.

Opdrachtnemer levert, configureert en beheert de netwerksensoren die voor de gevraagde dienstverlening noodzakelijk zijn. De geleverde netwerksensoren moeten passend te zijn qua capaciteit bij de gevraagde dienstverlening.

Security incidenten en data mogen niet verloren gaan, hiertoe is de geboden oplossing high-available en zijn maatregelen genomen om verlies van incidenten te voorkomen, ook bij bijvoorbeeld connectiviteitsproblemen, hacks en denial of service.

Opdrachtnemer houdt een auditlog bij welke continu en realtime is voor daartoe aangewezen medewerkers van Opdrachtgever. Hierin wordt in ieder geval met een timestamp opgenomen welke user welke informatie bekijkt dan wel muteert.

Correlatie van gegevens op basis van use-cases vindt realtime plaats en op basis van historische gegevens.

De SIEM-oplossing ondersteunt het aansluiten van feeds van zowel Windows, MacOS en Linux systemen/platformen.

De SIEM-oplossing ondersteunt ten minste de volgende typen logbronnen: end-points, netwerkmonitoring, syslogs, firewalls, mailservers, DNS, active directory, Identity and Access Management, antivirus, anti-DDOS, IDS/IPS en logdata van cloudserviceproviders.

De oplossing zoekt automatisch naar IoC's op basis van threat intelligence.

De SIEM oplossing moet werken op Microsoft 365 security, licentie E5 en daarnaast Fortinet-logging kunnen vertalen naar de SIEM-oplossing.

Vanuit health- and performancemanagement wordt continue inzichtelijk gemaakt of logbronnen normale activiteit/gedrag vertonen bij het aanleveren van data aan het SIEM.

Bij incidenten/meldingen wordt een classificatie gegeven, waarbij minimaal 3 classificatieniveaus worden gehanteerd.

De SIEM-oplossing moet in staat te zijn de event-tijd te corrigeren voor systemen met een onjuiste tijdaanduiding. De integriteit van de timestamp blijft hierbij gegarandeerd.

Verwerking van de loginformatie is (near) realtime.

Opdrachtnemer verzorgt 24/7 analyses van meldingen uit de aangesloten SIEM-oplossingen en geeft in geval van een (mogelijk) incident een mitigatieadvies aan de Opdrachtgever. Opvolging van incidenten buiten kantooruren (dus na 17.00 uur en voor 09.00 uur en in het weekend) moet enkel voor prio-1 meldingen plaatsvinden. Opdrachtgever heeft de mogelijkheid ook opvolging ten aanzien van andere meldingen buiten deze tijden af te nemen.

Meldingen worden gegenereerd op basis van classificaties.

Opdrachtgever kan in ieder geval via SMS, telefoon en email notificaties ontvangen betreffende verschillende classificaties van meldingen. Middels een interface kan een instelling hier voorkeuren voor opgeven en wijzigen.

Opdrachtnemer ondersteunt Opdrachtgever continu bij het minimaliseren van false positives en het finetunen van de dienstverlening.

(Technische) documentatie is opgesteld in de Nederlandse of Engelse (Cambridge Engels of vergelijkbaar niveau) taal.

Documentatie wordt continu up-to-date gehouden en de laatste versie wordt actief gedeeld met Opdrachtgever.

2. Logdata en event-data

De standaard retentietijd van log- en eventdata en het auditlog is 183 dagen.

Opdrachtgever kan de retentietijd naar eigen keuze verlengen en verkorten.

Data wordt dermate opgeslagen dat de integriteit en vertrouwelijkheid gegarandeerd is.

Het is binnen de oplossing mogelijk delen van de log- en eventdata te bevriezen waardoor dat specifieke deel van de data bewaard wordt tot het moment dat de bevriezing opgeheven wordt.

Opdrachtgever moet delen van de log- en eventdata kunnen exporteren en archiveren buiten het SIEM van de Opdrachtnemer.

Bij archivering van data wordt meta-data meegeleverd.

3. Informatiebeveiliging

Alle opslag en verwerking van data – ook die van eventuele subverwerkers – vindt plaats in de EU.

Opdrachtnemer gebruikt multi-factor authenticatie voor haar dienstverlening.

Alle data wordt versleuteld opgeslagen en versleuteld verstuurd.

4. Medewerkers

Opdrachtnemer stelt een vast team beschikbaar. Deze medewerkers beschikken over een HBO werk- en denkniveau, relevante werkervaring en goede kennis van de Nederlandse/ Engelse taal in woord en geschrift.

Opdrachtnemer garandeert dat gedurende de looptijd van de Overeenkomst de continuïteit in de dienstverlening gewaarborgd is. Tijdens ziekte, verlof en vertrek van de medewerkers van Opdrachtnemer beschikt Opdrachtnemer over mogelijkheden om gelijkwaardige gekwalificeerde medewerkers ter vervanging in te zetten.

Tijdens de uitvoering van de Overeenkomst wordt Opdrachtgever zo spoedig mogelijk geïnformeerd over:

- het vertrek dan wel de uitval van medewerker(s), ingezet op onderhavige opdracht;
- de wijze en termijn waarop de ontstane vacature zal worden ingevuld;
- de wijze waarop de continuïteit voor Opdrachtgever wordt gewaarborgd met warme overdracht van de medewerker met eventuele tijdelijke waarneming.

Vervanging van medewerkers van Opdrachtnemer leidt niet tot hogere kosten voor Opdrachtgever.

Wanneer medewerkers van de Opdrachtnemer naar oordeel van de Opdrachtgever niet over het vereiste HBO werk- en denkniveau, deskundigheid en ervaring beschikken, is de Opdrachtgever gerechtigd vervanging te eisen. Opdrachtgever heeft hiertoe een vetorecht.

Medewerkers van de Opdrachtnemer zijn gescreend op integriteit, waarbij de minimale eis is dat werknemer bij indiensttreding aan Opdrachtnemer een specifiek voor de functie geldende Verklaring omtrent Gedrag (VOG-verklaring) heeft overlegd, die bij indiensttreding niet ouder is dan 6 maanden.

5 SLA

Opdrachtnemer levert 24/7 dienstverlening voor opvolging (analyse en advisering) naar aanleiding van alerts die door de geleverde SIEM-oplossing worden gegenereerd ten aanzien van prio-1 melding.

Opdrachtnemer is tevens 24/7 telefonisch bereikbaar voor Opdrachtgever voor alle security incident gerelateerde vragen ten aanzien van deze meldingen.

De door Opdrachtnemer geleverde SIEM-dienst heeft een minimale beschikbaarheid van 99,0% gemeten op basis van een kalenderjaar.

Incidenten worden geclassificeerd. Bij de hoogste classificatie moet het mitigatie-advies binnen uiterlijk 45 minuten na melding van het event kenbaar gemaakt aan de Opdrachtgever.

Opdrachtnemer heeft bij Inschrijving een SLA gevoegd welke ten minste voldoet aan;

- heldere communicatiematrix;
- heldere escalatiematrix;
- duidelijke berekening beschikbaarheid en recovery time;
- duidelijke definities van classificaties met bijbehorende service levels.

6. Rapportage

Voor Opdrachtgever is het inzichtelijk welke bronnen aangesloten zijn op het SIEM, welke use-cases gebruikt worden, op welke IoC's gecontroleerd wordt en wat specifieke instellingen zijn (bv. welke thresholds ingesteld zijn).

Er is een zoekfunctie binnen de rapportages beschikbaar die door Opdrachtgever zelf gebruikt kan worden.

Er is sprake van multi-factor authenticatie voor toegang tot alle rapportages/portalen.

Opdrachtnemer stelt binnen 2 weken na afloop van de maand een digitale managementrapportage op. De managementrapportage omvat van de betreffende maand minimaal de volgende gegevens:

- beschrijving van de geconstateerde incidenten, problemen en calamiteiten;
- aangedragen oplossingen en de afhandeling van de incidenten;
- beschrijving hoe Opdrachtnemer invulling heeft gegeven aan de dienstverlening;
- beschrijving welke instrumenten door Opdrachtnemer zijn ingezet;
- overzicht klachten en klachtenafhandeling;
- overzicht van incidenten, problemen en calamiteiten;
- overzicht van endpoints langer dan 2 maanden niet actief.

De managementinformatie is immer in overeenstemming met de AVG.

7. Communicatie en evaluatie

Opdrachtnemer stelt één vaste contactpersoon (en een vervanger) beschikbaar, die primair verantwoordelijk is voor de naleving en verdere invulling van de Overeenkomst en die hiervoor als eerste aanspreekpunt

fungeert voor de Opdrachtgever. Deze contactpersoon (en vervanger) moet tijdens werkuren telefonisch en per e-mail bereikbaar te zijn en beheerst de Nederlandse-Engelse taal in woord en geschrift.

Opdrachtnemer beschikt over een helpdesk voor administratieve- en contractzaken, die beschikbaar is tussen 09.00 en 17.00 Nederlandse tijd.

De communicatie tussen Opdrachtgever en Opdrachtnemer vindt als volgt plaats:

Overleg	Opdrachtgever	Opdrachtnemer	Periodiciteit
Strategisch/tactisch	Manager Service en Ondersteuning CIO CISO		Bij implementatie en daarn eenmaal per halfjaar
Operationeel	Teamleider ICT dan wel aangewezen vervanger CISO		maandelijks

Op basis van de uitkomsten van het tactisch/strategisch overleg stelt Opdrachtnemer voor alle tekortkomingen en aandachtspunten en indien Opdrachtnemer en/of de Opdrachtgever dit wenselijk acht(en) verbeterplannen c.q. maatregelen op met als doel het doorlopend verbeteren van de uitvoering van de opdracht door Opdrachtnemer.

Voor alle overlegvormen geldt dat Opdrachtnemer zorg draagt voor de verslaglegging en verstrekt deze binnen vijf werkdagen als digitaal bestand (bewerkbare Microsoft Office applicatie of gelijkwaardig) per e-mail aan de Opdrachtgever.

Opdrachtgever evalueert per half jaar de dienstverlening met Opdrachtnemer.

De gedurende evaluatie gemaakte afspraken tussen partijen, zoals vastgelegd en overeengekomen in het gespreksverslag, heeft een bindend karakter, indien en voor zover deze afspraken niet strijdig zijn met afspraken in de Overeenkomst of tenzij partijen expliciet hebben aangegeven dat zij zich niet willen binden dan wel de aard van de afspraken verkennend/informatief zijn en geen bindend karakter hebben.

8. Klachtenregeling

Opdrachtnemer zorgt voor de ontvangst en registratie van alle klachten die betrekking hebben op deze Opdracht die schriftelijk, telefonisch of per e-mail zijn ingediend.

Opdrachtnemer is verantwoordelijk voor:

- het in behandeling nemen van alle klachten;
- afhandeling van alle gemelde klachten binnen 5 werkdagen;
- voorkoming van herhaling van klachten;

Van iedere klacht wordt door Opdrachtnemer geregistreerd:

- datum en tijd indiening klacht;
- afhandelingsdatum klacht;

- aard ingediende klacht;
- wijze en resultaat afhandeling klacht;
- wel of niet gegrondverklaring.

Periodiek vindt overleg plaats tussen Opdrachtgever en Opdrachtnemer waarin de klachten en de door Opdrachtnemer te nemen/genomen maatregelen worden besproken en geëvalueerd. Dit om klachten in de toekomst te voorkomen.

9. Overige verplichtingen

Opdrachtnemer garandeert dat hij en de eventueel door hem ingeschakelde derden voldoen en blijven voldoen aan alle wettelijke bepalingen en voorschriften en beschikken en blijven beschikken over alle vereiste vergunningen, beschikkingen en verklaringen ten aanzien van de dienstverlening en ondernemerschap.

10. Controle

Opdrachtgever is te allen tijde gerechtigd om de wijze van de uitvoering van deze Overeenkomst te controleren.

Opdrachtgever is gerechtigd alle mogelijke maatregelen te treffen die haar redelijk voorkomen. Eventuele kosten van de controles worden gedragen door Opdrachtgever, met uitzondering van de situatie waarin de Opdrachtnemer niet aan zijn verplichtingen blijkt te hebben voldaan. In dat geval worden de kosten gedragen door de Opdrachtnemer. Opdrachtnemer is slechts tot vergoeding van kosten gehouden voor zover de kosten aantoonbaar en redelijkerwijs gemaakt zijn.

11. Financieel

11.1 Prijzen

De prijs betreft de maandelijkse vergoeding voor de dienstverlening zoals vastgelegd in het programma van eisen alsmede eenmalige implementatiekosten.

Daarnaast kan gebruik gemaakt worden van de inhuur van personele capaciteit “consultant” van Opdrachtnemer tegen een vastgestelde uurprijs.

Alleen daadwerkelijk gewerkte uren van Opdrachtnemer worden gedeclareerd door Opdrachtnemer. Het aantal uren op jaarbasis kan wijzigen. Voor de inhuur van de uren geldt een jaarlijkse indexering, voor het eerst op 1 januari 2023 op basis van het CBS indexcijfer “CPI 2015=100 ” peildatum oktober.

De vermelde bedragen zijn met twee decimalen achter de komma, uitgedrukt in Euro’s en exclusief omzetbelasting (btw), tenzij duidelijk anders is vermeld.

Kosten die niet in de Inschrijving genoemd worden en niet verdisconteerd zijn in de aangeboden prijzen maar bij nader inzien noodzakelijk blijken te zijn voor een goed functioneren van de dienstverlening conform de gestelde eisen, zijn voor rekening van Opdrachtnemer.

11.2 Overige financiële condities

Het is niet toegestaan, zonder voorafgaande toestemming, om bijkomende kosten in rekening te brengen zoals maar niet beperkt tot overhead, administratie etc.

Alle bedragen zijn exclusief btw.

11.3 Facturering

Opdrachtnemer factureert de Opdrachtgever maandelijks achteraf door middel van een verzamelfactuur.

Op de factuur vermeldt Opdrachtnemer ten minste de volgende informatie:
• de wettelijk verplichte factuurgegevens, zoals vermeld op www.belastingdienst.nl > zakelijk > btw >administratie bijhouden > facturen maken > wettelijk verplichte gegevens;
• de naam en het adres van Opdrachtgever;
• contractnummer;
• volgnummer factuur;
• aantallen en prijzen;
• totaal in rekening gebrachte bedrag exclusief btw.

Opdrachtgever kan een vergelijking maken tussen het totaal door Opdrachtnemer gefactureerde bedrag en de door de Opdrachtgever goedgekeurde aantallen en prijzen. Opdrachtgever houdt zich het recht voor niet te betalen als er afwijkingen zijn.

De facturen worden, tenzij uitdrukkelijk anders is vermeld, gemaild in PDF format naar: inkoopfacturen@senzer.nl

11.4 Betalingsvoorwaarden

De betalingstermijn bedraagt 30 dagen na factuurdatum.

Overschrijding van (een) betalingstermijn(en) door de Opdrachtgever of niet-betaling door de Opdrachtgever van (een) factu(u)r(en) op grond van vermoede inhoudelijke onjuistheid van die factu(u)r(en) of van ondeugdelijkheid van de gefactureerde prestaties, geeft Opdrachtnemer niet het recht zijn prestaties op te schorten c.q. te beëindigen.

De Opdrachtgever geeft binnen de betaaltermijn van de factuur aan Opdrachtnemer aan indien de juistheid van de factuur in zijn geheel of gedeeltelijk wordt betwist. Alleen voor het betwiste gedeelte is de Opdrachtgever gerechtigd de betaling op te schorten. Het niet betwiste gedeelte van de factuur moet binnen de betaaltermijn te zijn voldaan. Het is Opdrachtnemer niet toegestaan creditnota’s te verrekenen met debet nota’s.

12. Gegevensoverdracht

Bij beëindiging van de Overeenkomst werkt Opdrachtnemer te allen tijde mee met Opdrachtgever om een zo efficiënt en effectieve mogelijke overgang te realiseren naar de nieuwe Opdrachtnemer. Het tijdig, voor einde van de Overeenkomst, beschikbaar stellen van de door Opdrachtgever of nieuwe Opdrachtnemer gevraagde documenten en gegevens maakt hier onderdeel van uit.