Samen aanjagen van vernieuwing

Bijlage 2 Programma van eisen

Inleiding

In deze bijlage worden de Eisen beschreven zoals die voor de gevraagde dienstverlening ter zake van SIEM-dienstverlening voor SURFsoc van toepassing zijn.

H1: Algemene eisen

Item	Omschrijving van de Minimumeis
A1	**Facturatie** Op de (digitale) factuur staat minimaal vermeld: a. Onderdeel of bestelnummer; b. Omschrijving geleverde diensten, of programmatuur en/of omschrijving van de uitgevoerde werkzaamheden inclusief vermelding van geïnstalleerde of onderhouden serienummers; c. Referentienummer of activiteitencode van SURF/Instelling; d. Naam Instelling; e. Naam van contactpersoon of afdeling van SURF/Instelling; f. Aantal; g. Orderdatum; h. Nettoprijs per stuk exclusief BTW; i. Netto totaalprijs per orderregel; j. Door SURF/Instelling aan te leveren bestelordernummer of werkordernummer; k. Bij implementatie en configuratiediensten aantal uren; l. Bij implementatie en configuratiediensten het netto uurtarief.
A2	**Service rapportage** U dient per maand, uiterlijk op de 15e Werkdag van de opvolgende maand, zowel in de richting van de individuele Instellingen als in de richting van SURF (overkoepelend) een schriftelijke rapportage in de Nederlandse taal te verzorgen vanuit uw helpdesk-registratiesysteem betreffende Incidenten, Problemen en Calamiteiten ten aanzien van de SIEM-dienst zelf.
A3	**Helpdesk Administratie en Contract** Opdrachtnemer beschikt over een Nederlandstalige helpdesk voor administratieve- en contractzaken, die beschikbaar is tussen 09.00 en 17.00 Nederlandse tijd.
A4	**Communicatie** Communicatie met Aanbestedende dienst en Instelling tussen 09:00 en 17:00 Nederlandse tijd, vindt plaats in de Nederlandse taal. Communicatie buiten deze uren (dus tussen 17:00 en 09:00) vindt plaats in de Nederlandse of Engelse (Cambridge Engels of vergelijkbaar niveau) taal.
A5	**Sleutelfunctionarissen** Opdrachtnemer stelt enkele sleutelfunctionarissen aan waaronder ten minste één vaste accountmanager inclusief een vervangend accountmanager, een Service Delivery Manager en een SOC-lead.
A6	**Documentatie** (Technische) documentatie is opgesteld in de Nederlandse of Engelse (Cambridge Engels of vergelijkbaar niveau) taal.
A7	**Documentatie** Documentatie wordt continu up-to-date gehouden en de laatste versie wordt actief gedeeld met SURF en Instellingen.

Met opmerkingen [SH1]: Aangepast n.a.v. ref. no. 41

H2: Eisen aan SIEM-Dienstverlening

Item	Omschrijving van de Minimumeis
S1	Opdrachtnemer biedt een SIEM-oplossing aan welke binnen de infrastructuur van SURF of binnen de infrastructuur van Opdrachtnemer wordt/is geplaatst waar meerdere Instellingen gebruik van kunnen maken in geval deze Instellingen geen SIEM-oplossing in de eigen infrastructuur wensen te plaatsen (multi-tenant oplossing).
S2	Opdrachtnemer biedt de SIEM-oplossing op basis van dezelfde techniek als in eis S1 voor plaatsing binnen de infrastructuur van een Instelling voor die Instellingen die op deze manier de SIEM-oplossing wensen af te nemen.
S3	Bij de multi-tenant oplossing is een strikte scheiding aangebracht is tussen alle data van Instellingen onderling, en tussen Instellingen en derden.
S4	Elke Instelling kan zelf zijn use-cases in richten, zijn eigen policies bepalen en zijn eigen thresholds instellen. Voor use-cases die zijn geleverd door Opdrachtnemer, verlopen wijzigingen via het door Opdrachtnemer vastgelegde change-proces.
S5	Use-cases en IoC's kunnen worden uitgewisseld tussen instellingen onderling en tussen instellingen en SURF.
S6	Opdrachtnemer biedt duidelijk gecontroleerd proces voor het doorvoeren van veranderingen en dient de mogelijkheid te hebben deze veranderingen te testen voordat ze in productie gaan.
S7	De geboden oplossing dient voldoende robuust te zijn om het benodigde volume aan logdata en events voor het totaal van Instellingen te kunnen afhandelen en daarin mee te kunnen op- en afschalen bij meer/minder gebruik van de dienst.
S8	De gevraagde diensten dienen eenvoudig, maandelijks, op- en afgeschaald te kunnen worden.
S9	De data binnen het geboden platform dient ook ingezet te kunnen worden voor andere doeleinden zoals IT-operations en Business Intelligence middels standaard API's of anderszins.
S10	Opdrachtnemer is verantwoordelijk voor levering, installatie, configuratie, beheer en onderhoud van de SIEM-oplossing
S11	Opdrachtnemer levert, configureert en beheert de netwerksensoren die voor de gevraagde dienstverlening noodzakelijk zijn. De geleverde netwerksensoren dienen passend te zijn qua capaciteit bij de gevraagde dienstverlening.
S12	Security incidenten en data mogen niet verloren gaan, hiertoe is de geboden oplossing high-available conform Eis D3 en zijn maatregelen genomen om verlies van incidenten te voorkomen, ook bij bijvoorbeeld connectiviteitsproblemen, hacks en denial of service.
S13	Opdrachtnemer houdt een auditlog bij welke continu en real-time individueel per instelling inzichtelijk is voor daartoe aangewezen medewerkers van desbetreffende Instelling en SURF. Hierin wordt in iedere geval met een timestamp opgenomen welke user welke informatie bekijkt dan wel muteert.
S14	Instellingen kunnen zelf searches, alerts en dashboards in het SIEM instellen, waarvan de uitkomst aan de Instelling zelf gestuurd wordt. In geval van gebruik van de multi-tenant oplossing mag dit via een change proces door Opdrachtnemer plaatsvinden.
S15	Use-cases kunnen per Instelling door geautoriseerde gebruikers van SURF en Instellingen ingesteld worden en gekopieerd naar andere Instellingen. Kopiëren van use-cases kan via een change-proces. Eigen use-cases kunnen door deze gebruikers zonder tussenkomst van een change-proces worden ingesteld.
S16	Correlatie van gegevens op basis van use-cases vindt real-time plaats en op basis van historische gegevens.
S17	Instellingen kunnen Out-of-the-box use-cases/correlatieregels afnemen zonder dat kosten worden berekend voor het gebruik van de betreffende use-case/correlatieregel.
S18	De SIEM oplossing ondersteunt het aansluiten van feeds van zowel Windows, MacOS en Linux systemen/platformen.

Met opmerkingen [SH2]: Aangepast n.a.v. ref. no. 8

Met opmerkingen [SH3]: Aangepast n.a.v. ref. no. 56.

Met opmerkingen [SH4]: Aangepast n.a.v. ref. no. 44

Met opmerkingen [SH5]: Aangepast n.a.v. ref. no. 257

Met opmerkingen [SH6]: Aangepast n.a.v. ref. no. 42

Item	Omschrijving van de Minimumeis
S19	De SIEM-oplossing ondersteunt ten minste de volgende typen logbronnen: end-points, netwerkmonitoring, syslogs, firewalls, mailservers, DNS, active directory, Identity and Access Management, anti-virus, anti-DDOS, IDS/IPS en logdata van cloudserviceproviders.
S20	De SIEM-oplossing biedt een mogelijkheid om niet-standaard platformen en logbronnen via een interface aan te sluiten.
S21	De SIEM-oplossing ondersteunt federatief inloggen via SURFconext, dat gebruik maakt van SAML2 en/of OpenID Connect[1].
S22	De SIEM-oplossing maakt gebruik van threat intelligence bronnen en additionele bronnen zijn via STIX/TAXII te koppelen.
S23	Threat intelligence die door SURF en/of een Instelling wordt aangeboden wordt opgenomen binnen de geboden oplossing, waaronder maar niet beperkt tot threat intelligence vanuit het Nationaal Detectie Netwerk (NDN).
S24	De oplossing zoekt automatisch naar IoC's op basis van threat intelligence. De resultaten hiervan worden getoond in de in H5 genoemde rapportages.
S25	Instellingen kunnen in de eigen logbestanden welke zich bevinden in de SIEM-oplossing, zoeken waa een hoge performance wordt geboden, conform onderstaande maximale zoektijden: Zoekperiode 1 dag – maximaal 10 seconden tot tonen resultaat; Zoekperiode 1 week – maximaal 60 seconden tot tonen resultaat; Zoekperiode 1 maand – maximaal 5 minuten tot tonen resultaat; en Zoekperiode 1 jaar – maximaal 15 minuten tot tonen resultaat.
S26	Vanuit health- and performancemanagement wordt continue inzichtelijk gemaakt of logbronnen normale activiteit/gedrag vertonen bij het aanleveren van data aan het SIEM.
S27	Bij incidenten/meldingen wordt een classificatie gegeven, waarbij minimaal 3 classificatieniveaus worden gehanteerd.
S28	De SIEM-oplossing dient in staat te zijn de eventtijd te corrigeren voor systemen met een onjuiste tijdaanduiding (bijvoorbeeld verkeerde tijdzone). De integriteit van de timestamp blijft hierbij gegarandeerd.
S29	Verwerking van de loginformatie is (near) real-time.
S30	Opdrachtnemer verzorgt 24/7 analyses van meldingen uit de aangesloten SIEM-oplossingen en geeft in geval van een (mogelijk) incident een mitigatieadvies aan de betreffende Instelling en brengt SURF hiervan op de hoogte. Opvolging van incidenten buiten kantooruren (dus na 17.00 uur en voor 09.00 uur en in het weekend) dient enkel voor prio-1 meldingen plaats te vinden. Instellingen hebben de mogelijkheid ook opvolging ten aanzien van andere meldingen buiten deze tijden af te nemen.
S31	Meldingen worden gegenereerd op basis van classificaties.
S32	Instellingen kunnen 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.
S33	De SIEM-oplossing voorziet in een geautomatiseerde koppeling bij SURF en Instellingen ten behoeve van integratie met een ticketingsysteem. De SIEM oplossing kan minimaal worden gekoppeld met: - Topdesk; - Jira; - ORTS. Een uni-directionele koppeling via bijvoorbeeld een e-mail volstaat.
S34	Bij meldingen van (mogelijke) incidenten dient een Instelling via een drill-down dieper op het incident in te kunnen gaan om het nader te kunnen onderzoeken.

Met opmerkingen [SH7]: Toegevoegd n.a.v. ref. no. 358.

Met opmerkingen [SH8]: Aangepast n.a.v. ref no. 52.

Met opmerkingen [SH9]: Aangepast n.a.v. ref. no. 53

[1] Meer informatie via deze link.

H3: Eisen aan logdata en eventdata

Item	Omschrijving van de Minimumeis
L1	De standaard retentietijd van log- en eventdata en het auditlog is 183 dagen.
L2	Instellingen kunnen de retentietijd (zie eis L1) naar eigen keuze verlengen en verkorten. Binnen de multi-tenant omgeving is de retentietijd voor alle hierop aangesloten Instellingen gelijk, en maximaal 183 dagen.
L3	Data wordt dermate opgeslagen dat de integriteit en vertrouwelijkheid gegarandeerd is.
L4	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.
L5	Instellingen dienen delen van de log- en eventdata te kunnen exporteren en te kunnen archiveren buiten het SIEM van de Opdrachtnemer.
L6	Bij archivering van data wordt meta-data meegeleverd.

Met opmerkingen [SH10]: Aangepast n.a.v. ref. no. 71.

H4: Eisen aan informatiebeveiliging

Item	Omschrijving van de Minimumeis
B1	Alle opslag en verwerking van data – ook die van eventuele subverwerkers – vindt plaats in de EER (Europese Economische Ruimte).
B2	Opdrachtnemer dient een geldig kwaliteitscertificaat te kunnen overleggen dat gebaseerd is op de ISO 27001 standaard voor informatiebeveiliging, inclusief de daarbij behorende verklaring van toepasselijkheid
B3	Opdrachtnemer dient een SOC2 type II verklaring of een ISAE3402 type 2 auditrapportage te overleggen, die beiden op het moment van Gunning niet ouder zijn dan één kalenderjaar. Indien Opdrachtnemer nog niet over deze bescheiden beschikt, dan dient hij deze uiterlijk 6 maanden na afronding van de initiële implementatie te overleggen.
B4	
B5	Opdrachtnemer gebruikt multi-factor authenticatie voor haar dienstverlening.
B6	Opdrachtnemer voldoet aantoonbaar aan de 8 STITCH eisen (zie Bijlage 14)
B7	Opdrachtnemer laat jaarlijks een pentest uitvoeren op zowel de multi-tenant omgeving als de single-tenant omgeving die gebruikt wordt binnen de infrastructuur van een Instelling door een onafhankelijke derde, en deelt de uitkomsten van deze pentest met Opdrachtgever.
B8	Alle data wordt versleuteld opgeslagen en versleuteld verstuurd.

Met opmerkingen [SH11]: Aangepast n.a.v. ref. no. 6

Met opmerkingen [SH12]: Verwijderd n.a.v. ref. no. 261.

H5: Eisen aan rapportages/portalen

Item	Omschrijving van de Minimumeis
P1	Opdrachtnemer biedt een rapportagefunctionaliteit welke via portalen bereikbaar is.
P2	De portalen zijn ook toegankelijk van buiten de infrastructuur van de betreffende Instelling.
P3	De rapportages worden geboden per aangesloten Instelling en er worden overall rapportages geboden aan SURF.
P4	Een Instelling en SURF moet 24/7 via een portaal informatie over meldingen en incidenten, opvolgingsadviezen en health- and performancemonitoring kunnen zien en raadplegen, inclusief de mogelijkheid om te kunnen zoeken. Onder health- and performancemonitoring wordt verstaan inzicht in zaken als resource gebruik, uptime van systeemonderdelen, beschikbaarheid van connectiviteit/verbindingen met aangesloten systemen en de hoeveelheid opgeslagen/verwerkte data in relatie tot de afgenomen licentie.
P5	SURF heeft inzage in de rapportages/portalen voor de aangesloten Instellingen en heeft toegang tot een specifieke rapportage waarin een geaggregeerd beeld wordt gegeven over alle aangesloten Instellingen heen.
P6	Voor een Instelling 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).
P7	Er is een zoekfunctie binnen de rapportages beschikbaar die door Instellingen en SURF zelf gebruikt kan worden.
P8	Er dienen – op verzoek - standaardrapportages geleverd te worden.
P9	Instellingen dienen maatwerkrapportages te kunnen instellen door standaardrapportages aan te passen. In geval dat een Instelling gebruik maakt van de SIEM-oplossing in haar eigen infrastructuur dient de Instelling tevens rapportages geheel op maat te kunnen maken.
P10	In geval dat een Instelling gebruik maakt van de SIEM-oplossing in haar eigen infrastructuur dient de Instellingen zelf rapportages te kunnen ontwikkelen o.b.v. queries die ze zelf instellen.
P11	Middels een interface kunnen Instellingen (zowel het geheel aan, als delen van de) gegevens van rapportages geautomatiseerd exporteren dan wel koppelen met andere systemen.
P12	Er is sprake van multi-factor authenticatie voor toegang tot alle rapportages/portalen.
P13	De rapportages omvatten de mogelijkheid om trendanalyses te kunnen uitvoeren.
P14	De rapportages bevatten een overzicht van het aantal: - Pogingen tot misbruik; - Datalekken.

Met opmerkingen [SH13]: Aangepast n.a.v. ref. no. 160

H6: Eisen aan implementatie

Item	Omschrijving van de Minimumeis
E1	Opdrachtnemer levert binnen 6 maanden na ingang van de Raamovereenkomst de gevraagde diensten op conform hetgeen is beschreven in Bijlage 1 bij het onderdeel implementatie en waarbij de dienst op dat moment voor productiedoeleinden gebruikt wordt door ten minste 5 Instellingen die gebruik maken van de oplossing in de eigen infrastructuur en daarbovenop van ten minste 10 Instellingen die gebruik maken van de multi-tenant oplossing.
E2	Opdrachtnemer toont binnen 6 maanden na ingang van de Raamovereenkomst aan dat de geboden oplossing aan alle vereisten conform dit PvE voldoet en Opdrachtnemer heeft hiertoe een test- en acceptatieprocedure, hierbij geldt dat de geboden oplossing end-to-end is getest en geaccepteerd inclusief benodigde service portalen.

Item	Omschrijving van de Minimumeis
E3	Opdrachtnemer is in staat om uiterlijk 6 maanden na ingang van de Raamovereenkomst ten minste 4 Instellingen per maand aan te sluiten op de dienstverlening.
E4	Opdrachtnemer ondersteunt Instellingen continu bij het minimaliseren van false positives en het fine-tunen van de dienstverlening.
E5	Opdrachtnemer levert binnen 3 maanden na ingang van de Raamovereenkomst een generiek implementatieplan op dat toegesneden is op het aansluiten van een Instelling op de geleverde oplossing.

H7: Eisen aan SLA

Item	Omschrijving van de Minimumeis
D1	Het service window voor de geleverde diensten is 24/7.
D2	Opdrachtnemer levert 24/7 dienstverlening voor opvolging (analyse en advisering) n.a.v. alerts die door de geleverde SIEM-oplossing worden gegenereerd ten aanzien van prio-1 melding. Opdrachtnemer is tevens 24/7 telefonisch bereikbaar voor SURF en Instellingen voor alle security incident gerelateerde vragen ten aanzien van deze meldingen.
D3	De door Opdrachtnemer geleverde SIEM-dienst heeft een minimale beschikbaarheid van 99,9% gemet op basis van een kalenderjaar, waarbij de maximale Recovery Time Objective (RTO) 240 minuten bedraagt. Decentrale componenten welke door Opdrachtnemer zijn geleverd, dienen uiterlijk de volgende werkdag vervangen te zijn.
D4	Incidenten worden geclassificeerd. Bij de hoogste classificatie dient het mitigatieadvies binnen uiterlijk minuten na melding van het event in het SIEM gemaakt zijn.
D5	Opdrachtnemer heeft bij Inschrijving een SLA gevoegd welke ten minste voldoet aan de gestelde eisen D1 t/m D4 en tevens bevat: - Duidelijke definities van terminologie; - Heldere communicatiematrix; - Heldere escalatiematrix; - Duidelijke berekening beschikbaarheid en recovery time; - Duidelijke definities van classificaties met bijbehorende service levels.

Met opmerkingen [SH14]: Aangepast n.a.v. ref. no. 52 en ref. no. 58.

Met opmerkingen [SH15]: Aangepast n.a.v. ref. no. 55.

H8: Eisen aan retransitie

Item	Omschrijving van de Minimumeis
R1	Op eerste aangeven van Opdrachtgever stelt Opdrachtnemer een specifiek exitplan op voor de Instelling(en).
R2	Ten tijde van de retransitie wordt de dienstverlening zoals overeengekomen voortgezet.
R3	Bij retransitie wordt alle data van een Instelling ter beschikking gesteld aan die Instelling of een door die Instelling of SURF aan te wijzen derde, inclusief bijbehorende meta-data.
R4	Na beëindiging van een Nadere overeenkomst verwijdert Opdrachtnemer alle data van de betreffende Instelling van haar systemen, tenzij hier andere afspraken over gemaakt worden (zoals het voor een bepaalde tijd nog bewaren van bepaalde data).

NB: Door ondertekening en bijvoegen van ondertekend programma van eisen, verklaart inschrijver akkoord te gaan met de eisen. Tevens verklaart inschrijver hiermee in staat te zijn de gevraagde dienstverlening conform programma van eisen uit te kunnen voeren.

Ondertekening
Naam inschrijver:
Naam tekenbevoegde:
Functie tekenbevoegde: