Bijlage 6 - Programma van Eisen SIEM-SOC

De opdrachtnemer moet voldoen aan de gestelde eisen - en bij voorkeur aan de gestelde wensen - in bijgaand Programma van Eisen (PvE).

De relevantie van de eis/wens wordt aangegeven in de kolom "Categorie", met de volgende mogelijkheden:
H Hardware, apparatuur.

A Applicatie die door de opdrachtgever op eigen systemen wordt geinstalleerd en beheerd (aanname: alleen toegankelijk via het interne netwerk).

W Als A toegankelijk is via een web-interface.

S SaaS-applicaties die door de opdrachtnemer worden beheerd en op systemen van de opdrachtnemer zijn geïnstalleerd en die toegankelijk zijn via het internet als webapplicatie.

D Delen van persoonsgegevens of andere gegevens met opdrachtnemers, die zelf verantwoordelijk zijn in de zin van de AVG (bv. aannemers, uitgever van een personeelsblad). NB: een applicatie/platform voor uitwisseling van deze gegevens moet voldoen aan de eisen van de categorie W.

Nr.	Omschrijving Eis/Wens	Categorie	Eis/Wens/NvT
1. Algemeen			
1.1.	De opdrachtnemer levert een volledig gehoste SaaS-oplossing. Het beheersysteem binnen de SaaS-oplossing is een web based oplossing en de front-end voor de medewerkers van de opdrachtgever bestaat uit een webapplicatie. De ICT-prestatie wordt beheerd in een datacenter van de opdrachtnemer. Een eventuele logconnector mag wel on premises.	S	Eis
1.2.	De opdrachtnemer garandeert de levering, implementatie, onderhoud, gebruiksrecht en doorontwikkeling van de applicatie gedurende de contractperiode, inclusief alle nieuwe (standaard) functionaliteiten en wettelijke wijzigingen. Enige uitzondering hierop is een functionaliteit die niet in scope is van deze aanbesteding en seperaat wordt aangeschaft gedurende de contractperiode.	AWS	Eis
1.3.	Hosting betreft een voldoende beveiligde fysieke en logische omgeving – bestaande uit alle benodigde software (zoals virtualisatiesoftware, firewalls, technisch beheertooling en back-upsoftware) en hardware (zoals serverapparatuur, opslag, back-upapparatuur en netwerken) – beschikbaar stellen van een toegangsbeheersysteem, inclusief het uitvoeren van het (technisch) beheer van deze omgeving.	S	Eis
1.4.	Onderdeel van de hosting is tevens de connectiviteit (dataverbinding, bandbreedte) van de applicatie richting de opdrachtgever (t.b.v. medewerkers, koppelingen, etc.). Ook het opzetten van beveiligde verbindingen t.b.v. de koppelingen is onderdeel van de hosting.	S	Eis
1.5.	Het systeem is volledig in het Nederlands in woord en geschrift.	HAWS	Wens
1.6.	De opdrachtnemer stelt een Nederlandstalige handleiding (bedieningsprocedures) voor de medewerkers van de opdrachtgever ter beschikking.	HAWS	Eis
2. Authenticatie dmv EntraID			
2.1.	Toegang verloopt via Microsoft Entra ID van de opdrachtgever	WS	Eis
2.2.	Het systeem ondersteunt Single Sign On (SSO).	AWS	Eis
2.3.	Sessies kunnen automatisch worden afgesloten na een in te stellen periode van inactiviteit.	AWS	Eis
3. Autorisatie			
3.1.	Autorisatie van gebruikers is op basis van rollen in te stellen (RBAC, Role Based Access Control). Hierbij wordt rekening gehouden met het 'least privilige' en 'need-to-know' principe.	AWS	Eis
3.2.	Functioneel beheerders kunnen rollen en de autorisaties van rollen inrichten en beheren.	AWS	Eis
3.3.	De applicatie heeft een rapportage waarin alle gebruikers die toegang hebben tot het systeem zijn opgenomen met hun actuele rol(len) en autorisatie(s).	AWS	Wens
3.4.	De toewijzing van onverenigbare rollen kan worden verhinderd, gesignaleerd of gerapporteerd (functiescheiding).	AWS	Wens
3.5.	De applicatie draait onder serviceaccounts (niet onder een algemeen beheeraccount, zoals root- of (local- of domain-)administrator). Serviceaccounts krijgen alleen de specifieke rechten die nodig zijn en kunnen niet gebruikt worden om in te loggen.	AWS	Eis
3.6.	De bevoegde personen die vanuit opdrachtnemer toegang krijgen tot de oplossing wordt tot een minimum beperkt en kan middels logfiles overlegd worden. Desbetreffende medewerkers beschikken over een VOG en werken volgens de gedragsregels van de opdrachtgever.	AWS	Eis
4. Logging			
4.1.	De volgende gebeurtenissen worden gelogd: - Gebruik van technische beheerfuncties, zoals (succesvol en onsuccesvol) een backup maken, overschrijven of wissen van logfiles, uitgeven en intrekken van certificaten/encryptiesleutels; - Gebruik van functionele beheerfuncties, zoals het wijzigen van instellingen (bv. systeemtijd), updates van de applicatie; - Handelingen van autorisatiebeheer, zoals het aanmaken, blokkeren en verwijderen van gebruikers, wachtwoord reset, het aanpassen, toekennen en intrekken van autorisaties; - Handelingen van gebruikers, zoals het raadplegen van bestanden, uitvoeren van acties in een applicatie; - Inlogpogingen zowel succesvol als onsuccesvol worden vastgelegd; - Foutmeldingen van applicaties, zoals poging tot overschrijding van geautoriseerde bevoegdheden (melding "Access Denied"), overschrijding van drempelwaarden in gebruik of belasting van systeemhulpbronnen.	AWS	Eis
4.2.	Logginggegevens kunnen aan een centrale loggingserver worden geleverd.	AWS	Eis
4.3.	Een logregel bevat minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis.	AWS	Eis
4.4.	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	AWS	Eis
4.5.	De bewaarperiode van log-entries is instelbaar.	AWS	Eis
4.6.	Logginggegevens zijn door een functioneel beheerder zonder tussenkomst van de opdrachtnemer te raadplegen. Logbestanden kunnen niet door een functioneel beheerder worden verwijderd of aangepast.	AWS	Eis
5. Configuratie en overige			
5.1.	De applicatie is bruikbaar op apparaten met het Windows 10 en hoger operating system, ook als het Windows operating systeem is gevirtualiseerd (VDI). Indien ook beschikbaar op IOS (iPad en iPhone) past de weergave van de applicatie zich aan het soort apparaat aan.	AWS	Eis
5.2.	De applicatie maakt geen gebruik van onveilige (web)plugins zoals van Java, Flash en Silverlight.	AWS	Eis
5.3.	De applicatie is alleen toegankelijk via versleutelde HTTPS/TLS 1.3 verbinding en uitgebreide validatie certificaat (Extended Validation SLL). Eerdere versies van TLS support zijn uitgeschakeld.	WS	Eis
5.4.	De applicatie dwingt HTTPS af door middel van HTTP Strict Transport Security (HSTS, RFC 6797).	WS	Eis
5.5.	De applicatie is toegankelijk en compatible met de meest recente Microsoft Edge webbrowser, maximaal twee versies lager.	WS	Eis
5.6.	De applicatie voorziet in het gebruik van de cookie attributen ‘HttpOnly’ en ‘Secure’.	WS	Eis
5.7.	De applicatie valideert alle invoer, gegevens die aan de applicatie worden aangeboden, aan de serverzijde.	AWS	Eis
5.8.	De applicatie voldoet aan de ICT Beveiligingsrichtlijnen voor transport layer security van het NCSC.	S	Eis
5.9.	De applicatie heeft een Qualis rating A of beter (te testen via https://www.ssllabs.com/ssltest/).	S	Eis
5.10.	De opdrachtnemer ondersteunt de standaarden uit de pas-toe-of-leg-uit lijst van het Forum Standaardisatie van de Nederlandse overheid (https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht).	HAWS	Eis

5.11.	Gegevens worden versleuteld of gehashed opgeslagen, dit geldt zowel voor data-at-rest (fysieke opslagmedia, operationeel en backups) als data-in-transit (netwerkverbindingen).	S	Eis
5.12.	De website moet zowel via IPv4 als IPv6 benaderbaar zijn.	WS	Eis
5.13.	Niet gebruikte protocollen/IP-poorten kunnen worden afgesloten (bijv. SMNP).	S	Wens
5.14.	Niet gebruikte softwarecomponenten worden verwijderd (hardening, bijvoorbeeld Powershell).	S	Wens
5.15.	Niet benodigde rechten van accounts worden ingetrokken, met bijzondere aandacht voor beheerders- en serviceaccounts.	S	Eis
5.17.	Voor DNS moet DNSSEC worden gebruikt.	S	Eis
6. Backup en gegevensbeheer			
6.1.	Er kan een backup gemaakt worden van de data terwijl de applicatie toegankelijk blijft voor gebruikers.	AWS	Eis
6.2.	Backups worden periodiek uitgevoerd. Tenzij anders overeengekomen bedraagt het maximale dataverlies (RPO) 24 uur en de maximale hersteltijd (RTO) 16 werkuren.	S	Eis
6.3.	Backups worden bewaard op een locatie waarbij een voorval op de productielocatie niet kan leiden tot een schade op de backuplocatie en andersom.	S	Eis
6.4.	De oplossing ondersteunt configureerbare bewaartermijnen voor back-ups conform continuïteits-, compliance- en beveiligingseisen	S	Eis
6.5.	De restoreprocedure wordt minimaal jaarlijks getest.	S	Eis
6.6.	De oplossing ondersteunt bewaarbeleid voor audit- en securitylogs conform wettelijke en organisatorische eisen.	AWS	Eis
6.7.	Data moet gemakkelijk ontsloten kunnen worden voor rapportagedoeleinden.	S	Eis
6.8.	De gegevens van opdrachtgever worden alleen opgeslagen en verwerkt in Europa of binnen de EER, in overeenstemming met de eisen van de AVG.	S	Eis
7. Softwareontwikkeling			
7.1.	De opdrachtnemer hanteert het principe van security by design, security by default, privacy by design en privacy by default.	AWS	Eis
7.2.	Alle wijzigingen worden door de opdrachtnemer altijd eerst getest in een OTA-omgeving voordat deze in productie worden genomen.	AWS	Eis
7.3.	Wanneer een nieuwe release beschikbaar komt worden de releasenotes binnen één week beschikbaar gesteld.	AWS	Wens
7.4.	De opdrachtnemer hanteert bij de softwareontwikkeling de OWASP secure coding practices conform de Quick reference guide (https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf).	WS	Wens
7.5.	De opdrachtnemer verifieert software van derden die wordt opgenomen in de software van de opdrachtnemer op de aanwezigheid van kwaadaardige code, voor elke versie die wordt opgenomen in de software.	AWS	Eis
8. Technisch beheer			
8.1.	Technisch applicatiebeheer wordt geheel verzorgt door opdrachtnemer, dit betreft de werkzaamheden die nodig zijn voor het waarborgen van de ononderbroken goede werking van de SaaS-oplossing en het beheersysteem.	S	Eis
8.2.	Technisch applicatiebeheer omvat tevens het continu en actief monitoren van o.a. de beschikbaarheid, capaciteit, continuïteit, back-up, beveiliging en data-integriteit van het beheersysteem.	S	Eis
8.3.	Het door de opdrachtnemer geleverde beheersysteem dient te worden uitgevoerd in een TAPU-architectuur (test, acceptatie, productie en uitwijk). Dit dient minimaal twee separate omgevingen te betreffen, waarin de test- en productie omgeving van elkaar gescheiden zijn (bijvoorbeeld P en TAU). Alle benodigde licenties om dit te realiseren dienen aangeboden te worden.	S	Eis
8.4.	De test- en acceptatieomgeving zijn inzetbaar met behulp van geanonimiseerde gegevens.	AWS	Eis
8.5.	Er wordt geen gebruik gemaakt van onbeveiligde of publieke internetverbindingen. Uitzondering hierop kan zijn een met de opdrachtgever afgesproken beveiligde uitwijkverbinding over het publieke internet om calamiteiten op te vangen.	AWS	Eis
9. Informatiebeveiliging			
9.1.	De opdrachtnemer is ISO27001 gecertificeerd (ISO27017 voor cloud-diensten) of vergelijkbaar, mits aantoonbaar op basis van een externe audit. De opdrachtnemer toont dit jaarlijks opnieuw aan door het aanleveren van een certificaat en Verklaring van Toepasselijkheid (VvT).	SD	Eis
9.2.	De opdrachtnemer beschikt over privacy- en informatieveiligheidsbeleid.	AWSD	Eis
9.3.	De opdrachtnemer garandeert dat er binnen de organisatie iemand is benoemd om de informatiebeveiliging te waarborgen.	AWSD	Eis
9.4.	Bestuurders van de opdrachtnemer beschikken over een certificaat waaruit blijkt dat zij een training hebben gevolgd om informatiebeveiligingsrisico's en beheersmaatregelen te kunnen beoordelen.	AWSD	Eis
9.5.	De opdrachtnemer laat periodiek vulnerability analyses of penetratietesten uitvoeren door een externe onafhankelijke partij. Een samenvatting van de resultaten wordt gedeeld met de opdrachtgever.	S	Wens
9.6.	IT-voorzieningen en apparatuur bij opdrachtnemer zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen.	SD	Eis
9.7.	De opdrachtnemer beschikt over jaarlijks geteste uitwijk- en continuiteitsplannen om de dienstverlening in het geval van rampen binnen 24 uur te kunnen hervatten.	S	Eis
9.8.	De opdrachtnemer voorziet in (gratis) patches en updates voor de software, firmware en drivers om deze actueel en veilig te houden gedurende de verwachte gebruiksduur van de software/hardware.	HAWS	Eis
9.9.	De opdrachtnemer voldoet aan de ICT-beveiligingsrichtlijnen voor Webapplicaties van het NCSC.	WS	Eis
9.10.	Ter bescherming tegen malware behoren beheersmaatregelen te worden geïmplementeerd voor detectie, preventie en herstel.	HAWS	Eis
9.11.	De opdrachtnemer heeft een logging- en monitoringsfunctie (SIEM/SOC) geïmplementeerd voor de oplossing. Opdrachtnemer geeft opvolging aan informatiebeveiligingsgebeurtenissen en communiceerd in lijn met de urgentie/impact met het CERT van opdrachtgever.	S	Eis
9.12.	De opdrachtnemer heeft een Coordinated Vulnerability Disclosure (CVD)-procedure ingericht en gepubliceerd.	S	Eis
9.13.	De opdrachtnemer garandeert dat ongeautoriseerde personen geen toegang hebben tot gegevens of gegevensdragers (zoals harde schijven en back-upmedia) die tussentijds of na beëindiging van de overeenkomst worden verwijderd c.q. worden vervangen.	S	Eis
9.14.	De opdrachtnemer vrijwaart de opdrachtgever voor inbreuk op rechten van derden wanneer software van derden wordt opgenomen in de software van de opdrachtnemer.	AWS	Eis
9.15.	De opdrachtnemer levert technische architectuurplaten van de SaaS-oplossing en houdt deze gedurende de overeenkomst actueel.	S	Eis
9.16.	Wijzigingen in de dienstverlening /functionaliteit en de consequenties voor gebruikers worden ten minste drie maanden voorafgaand aan de inwerkingtreding gemeld aan opdrachtgever.	AWSD	Wens
9.17.	De opdrachtgever wordt in de gelegenheid gesteld om functionele wijzigingen in de applicatie vóór de implementatie te testen.	S	Wens
9.18.	Functionele of andere beperkingen worden ten minste een halfjaar van tevoren gemeld. Te denken valt ook aan het beëindigen van de ondersteuning van bepaalde hardware- (paslezers) of softwareversies (zoals browsers).	AWS	Eis
9.19.	De opdrachtnemer geeft vooraf en bij wijzigingen inzage in de naam, aard afgenomen dienst en de uitbestede verwerkingen van toeleveranciers (bv. een datacenter, hostingpartij) en eventuele risico's in de keten van toeleveranciers.	S	Eis
9.20.	De opdrachtnemer garandeert dat afspraken tussen opdrachtgever en opdrachtnemer over informatiebeveiliging of gelijkwaardige afspraken ook van toepassing zijn op de toeleveranciers van de opdrachtnemer en dat daarmee het overeengekomen beveiligingsniveau tussen opdrachtgever en opdrachtnemer in de gehele keten is gewaarborgd.	S	Eis
9.21.	De opdrachtnemer meldt kwetsbaarheden, ook van toeleveranciers, aan opdrachtgever zodra deze bekend zijn. De blootstelling aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.	AWSD	Eis
9.22.	De opdrachtnemer gaat akkoord met de algemene voorwaarden van de opdrachtgever. Algemene voorwaarden opdrachtnemer zijn uitgesloten.	HAWS	Eis
9.23.	De opdrachtnemer verleent alle noodzakelijke medewerking aan de uitvoering van (wettelijke verplichte) audits.	AWS	Eis
9.24.	De opdrachtgever heeft het recht om een onafhankelijke externe audit uit te laten voeren bij opdrachtnemer ter validatie van aangeleverde rapportages.	AWS	Eis
10. Privacy			
10.1.	De opdrachtnemer houdt zich aan de naleving van alle wetgeving (Nederlandse en Europese) aangaande privacybescherming m.b.t. de door hem geleverde oplossing en diensten.	HAWSD	Eis

10.2.	Tussen de opdrachtgever en opdrachtnemer wordt na gunning een verwerkersovereenkomst afgesloten op basis van het VNG/IBD formaat welke de opdrachtgever hanteert.	S	Eis
10.3.	De opdrachtnemer garandeert dat opdrachtgever te allen tijde eigenaar blijft van de informatie die wordt verwerkt in de applicatie.	AWS	Eis
10.4.	Zonder wettelijke verplichting of gerechtelijke bevel worden door opdrachtnemer geen gegevens met andere partijen dan opdrachtgever gedeeld. Opdrachtgever wordt tijdig geïnformeerd wanneer aan voorwaarden wordt voldaan en een andere partij toegang krijgt tot gegevens.	AWSD	Eis
10.5.	De opdrachtnemer faciliteert de uitoefening van de rechten van betrokkenen. Het is mogelijk om een kopie van de verwerkte persoonsgegevens in een gangbare elektronische vorm te genereren en verstrekken en onjuiste persoonsgegevens aan te passen.	S	Eis
10.6.	De opdrachtnemer meldt incidenten, waaronder datalekken, binnen 24 uur. Opdrachtnemer verstrekt aan opdrachtgever de vermoedelijke oorzaak, gevolgen en contactgegevens verantwoordelijk functionaris. Significante incidenten worden gemeld bij het CSIRT en de toezichthouder(s).	SD	Eis
10.7.	De opdrachtnemer heeft een aantoonbaar beschreven en vastgesteld proces voor incidenten en datalekken.	AWSD	Eis
10.8.	De opdrachtnemer verleent medewerking aan onderzoek door de gemeente of het CSIRT na een incident.	AWSD	Eis
10.9.	Op verzoek van opdrachtgever werkt opdrachtnemer mee aan het opstellen van een (pre-)DPIA (Data Protection Impact Assessment) en verricht opdrachtnemer eventuele wijzigingen om risico's te mitigeren.	SD	Eis
10.10.	Bij toepassing van algoritmes en/of kunstmatige intelligentie (AI) in geleverde oplossing, dient opdrachtnemer vooraf transparant te zijn richting opdrachtgever. Opdrachtnemer levert een verklaring aan met voldoende informatie waarmee publicatie in het algoritmeregister door de opdrachtgever gerealiseerd kan worden.	AWSD	Eis
11. Beschikbaarheid (eisen kunnen ook zijn opgenomen in een SLA)			
11.1.	De SaaS-oplossing is 99% beschikbaar. (3d 15h 39m 30s uitval)	S	Eis
11.2.	De opdrachtnemer zorgt ervoor dat opdrachtgever niet afhankelijk is en geen last heeft van (het gedrag van) andere afnemers, zowel nu als in de toekomst, in geval van: performance, technische uitwijk of bij onderhoud- en releasewerkzaamheden.	S	Wens
11.3.	Onderhoudstijden van opdrachtnemer vinden plaats na werktijd (17:00-8:00), in de avonden, weekenden en op nationale feestdagen.	AWS	Eis
11.4.	De opdrachtnemer hanteert een vast jaarlijks update-, upgrade- en patchschema.	AWS	Eis
11.5.	Werkzaamheden door de opdrachtnemer worden altijd minimaal 14 werkdagen van tevoren gecommuniceerd.	AWS	Eis
11.6.	Een uitzondering op punten 11.2, 11.3, 11.4 en 11.5 zijn calamiteiten met een hoge prioriteit zoals onvoorziene zaken waarbij de integriteit van de gegevens in gevaar zijn, informatieveiligheidsincidenten en rampen.	AWS	Eis
11.7.	Bij verstoringen/incidenten is de volgende prioriteitsindeling van toepassing: - Kritiek: het incident heeft vergaande en onmiddellijke invloed op de werking van de SaaS-oplossing. Alle gebruikersgroepen kunnen niet meer werken met het systeem. - Hoog: het incident heeft aanzienlijke invloed op de werking van de SaaS-oplossing en is productie verstorend. Dit is een incident waardoor een bepaalde groep gebruikers niet kan werken met één of meer functionaliteiten binnen het systeem. - Middel: het incident heeft aanzienlijke invloed op de werking van de SaaS-oplossing en is productie verstorend. Dit is een incident waardoor er door één specifieke gebruiker niet gewerkt kan worden met één of meer functionaliteiten (of een onderdeel daarvan). - Laag: het incident heeft minimale invloed op de werking van de SaaS-oplossing en is niet productieverstorend.	S	Eis
11.8.	Meldingen van verstoringen/incidenten worden door de opdrachtnemer binnen onderstaande normen afgehandeld: - Kritiek: reactietijd 30 minuten, hersteltijd 2 uur. - Hoog: reactietijd 1 uur, hersteltijd 4 uur. - Middel: reactietijd 4 uur, hersteltijd 8 uur. - Laag: reactietijd 8 uur, hersteltijd 40 uur.	S	Eis
11.9.	Medewerkers van opdrachtnemer bieden ondersteuning in de Nederlandse taal in woord en geschrift.	AWS	Eis
11.10.	De opdrachtnemer beschikt over een helpdesk welke medewerkers van de opdrachtgever van maandag tot en met vrijdag van 8:00 tot 17:00 per telefoon te woord kan staan.	AWS	Eis
11.11.	De opdrachtnemer kan op verzoek gedurende de dienstverlening en na afloop van de dienstverlening gegevens die berusten bij de opdrachtnemer permanent en aantoonbaar wissen, inclusief de koppeling naar een kopie of reproductie.	AWS	Eis
11.12.	De opdrachtnemer heeft een exit-procedure opgesteld.	AWS	Eis
11.13.	Jaarlijks vindt een evaluatie plaats tussen opdrachtgever en opdrachtnemer.	AWS	Eis
12. Koppelingen en delen van informatie			
12.1.	De opdrachtnemer organiseert de afstemming en realisatie van de koppelingen (gegevensuitwisseling) met andere noodzakelijke applicaties van de opdrachtgever. De opdrachtgever heeft een ondersteunende rol.	S	Eis
12.2.	Systeemkoppelingen zijn verstleuteld met AES-256 of vergelijkbaar.	S	Eis
12.3.	Systeemkoppelingen zijn geauthentiseerd met API tokens van 256 bit of wachtwoorden van ten minste 20 tekens.	S	Eis
12.4.	De SaaS-oplossing ondersteunt gangbare uitwisselformaten als XML, TXT, CSV, PDF-A, etc.	S	Eis
13. Aanvullende eisen			
13.1.	Koppeling met onze ITSM/FMIS facilitor (email, api, of anders)		Wens
13. Aanvullende eisen (optionele dienstverlening)			
13.2	De opdrachtnemer moet de dienst reactieve incidentbehandeling als optionele module aanbieden, die door opdrachtgever in op een later moment zou kunnen worden afgenomen.		Eis
13.3	De opdrachtnemer moet alle door het SIEM/SOC gedetecteerde of door opdrachtgever gemelde security incidents reactief behandelen conform NEN-ISO/IEC 27035 of een gelijkwaardig erkend raamwerk.		Eis
13.4	De opdrachtnemer moet 24x7 beschikbaar zijn voor detectie, triage en behandeling van security incidents.		Eis
13.5	De opdrachtnemer moet elk incident registreren in een ticketing-/casemanagementsysteem met minimaal: uniek incidentnummer, tijdstempels (detectie, melding, start behandeling, afsluiting), classificatie, prioriteit, betrokken assets, uitgevoerde acties en status.		Eis
13.6	De opdrachtnemer moet incidenten primair registreren in het ticketingsysteem van de opdrachtgever, dan wel in samenspraak een gelijkwaardig alternatief overeenkomen.		Eis
13.7	De opdrachtnemer moet een bidirectionele, geautomatiseerde koppeling realiseren tussen het SIEM/SOC-platform en het ticketingsysteem van opdrachtgever, zodat tickets, statuswijzigingen, bijlagen en afhandelingsnotities automatisch worden gesynchroniseerd.		Eis
13.8	De opdrachtnemer moet voor P1-incidenten (kritiek) een eerste melding doen binnen 15 minuten en een basisrapportage leveren binnen 1 uur, 24x7 gerekend vanaf detectie of melding.		Eis
13.9	De opdrachtnemer moet voor P2-incidenten (hoog) een eerste melding doen binnen 30 minuten en een basisrapportage leveren binnen 4 uur.		Eis
13.10	De opdrachtnemer moet voor P3-incidenten (middel) een eerste melding doen binnen 2 uur en een basisrapportage leveren binnen 8 werkuren.		Eis
13.11	De opdrachtnemer moet voor P4-incidenten (laag) een eerste melding doen binnen 1 werkdag en een basisrapportage leveren binnen 2 werkdagen.		Eis
13.12	De opdrachtnemer moet bij elk incident een basisrapportage aanleveren aan opdrachtgever binnen de in eisen 13.8 t/m 13.11 genoemde termijnen.		Eis
13.13	De opdrachtnemer moet in de basisrapportage minimaal opnemen: incidentnummer, classificatie en prioriteit, datum en tijdstip van detectie, melding en start behandeling, status van de melding aard en korte omschrijving van het incident, detectiebron (use case, regel, sensor of melder), betrokken assets, gebruikers, IP-adressen en/of locaties, vermoedelijke oorzaak en, indien bekend, attack vector en MITRE ATT&CK-mapping, reeds uitgevoerde acties door SOC, concreet advies voor vervolgacties door opdractgever, inclusief urgentie, Indicators of Comproise (IoC's), waar van toepassing.		Eis