Bijlage 7 – Marktconsultatieverslag SIEM, SOC, SOAR-dienstverlening

Ten behoeve van Veiligheidsregio Noord- en Oost-Gelderland

Inleiding

Veiligheidsregio Noord- en Oost-Gelderland (hierna: VNOG) heeft een marktconsultatie uitgevoerd voor SIEM-, SOC- en SOAR-dienstverlening. Naar aanleiding van de publicatie hebben negentien (19) partijen een reactie ingediend. Dit verslag bevat een samenvatting van de schriftelijke beantwoording van de gestelde vragen en geeft een geaggregeerd beeld van de inzichten die uit deze reacties naar voren zijn gekomen.

Vanwege het grote aantal reacties is ervoor gekozen een representatieve selectie van vijf (5) marktpartijen uit te nodigen voor een verdiepend gesprek. Daarbij is gekeken naar de toegevoegde waarde voor het verkrijgen van een zo volledig mogelijk marktbeeld. De gesprekken hebben plaatsgevonden op donderdag 18 juni 2026 en donderdag 25 juni 2026.

De verdiepende gesprekken maakten onderdeel uit van de marktverkenning en hadden als doel de ontvangen antwoorden nader toe te lichten en beter inzicht te verkrijgen in de mogelijkheden die de markt biedt. De selectie van partijen voor deze gesprekken is uitsluitend gemaakt vanuit dit doel en zegt niets over de geschiktheid of voorkeur voor bepaalde marktpartijen.

Ten tijde van de marktconsultatie bevond een eventuele aanbestedingsprocedure zich nog in de voorbereidingsfase. Deelname aan een verdiepend gesprek leverde geen voordeel op bij een eventuele toekomstige aanbestedingsprocedure. Alle marktpartijen krijgen daarbij gelijke kansen en zullen worden beoordeeld op basis van de op dat moment geldende aanbestedingsstukken en criteria.

Thema 1: Organisatie en ervaring

De deelnemende marktpartijen bestaan voornamelijk uit gespecialiseerde cybersecuritydienstverleners met ervaring in SOC-, SIEM-, MDR- en aanverwante securitydiensten voor organisaties binnen de vitale en publieke sector. Daarbij worden onder meer referenties genoemd binnen de overheid, zorg, energie-, water- en veiligheidssector. Meerdere partijen geven aan ervaring te hebben met organisaties waar continuïteit, beschikbaarheid en crisisbeheersing een belangrijke rol spelen.

Vrijwel alle partijen geven aan de kern van de dienstverlening zelf uit te voeren. Dit betreft onder andere monitoring, detectie, analyse, incidentcoördinatie, threat hunting en het beheer van detectieregels. Voor specialistische onderdelen, zoals threat intelligence, digitale forensics of incident response, wordt regelmatig samengewerkt met externe kennis- en technologiepartners.

Partijen verschillen in de wijze waarop zij hun dienstverlening organiseren. Waar sommige partijen kiezen voor volledige uitvoering in eigen beheer, maken andere partijen gebruik van een netwerk van gespecialiseerde samenwerkingspartners. Daarbij wordt door vrijwel alle partijen benadrukt dat de regie, verantwoordelijkheid en communicatie richting de opdrachtgever eenduidig zijn ingericht.

Daarnaast wijzen meerdere partijen op het belang van Europese datasoevereiniteit, transparante ketensamenwerking en duidelijke verantwoordelijkheidsverdeling binnen de dienstverlening.

Thema 2. Dienstverlening en Oplossingsrichting

De marktpartijen hanteren overwegend een gefaseerde implementatieaanpak. Voor standaardomgevingen wordt een eerste operationele dienstverlening doorgaans binnen zes tot twaalf weken gerealiseerd. De uiteindelijke doorlooptijd is afhankelijk van factoren zoals de omvang van de omgeving, het aantal logbronnen, de aanwezigheid van OT-systemen en de beschikbaarheid van benodigde informatie vanuit de opdrachtgever. Meerdere partijen benadrukken het belang van voldoende tijd voor inrichting en tuning om de kwaliteit van detectie en respons te waarborgen.

Vrijwel alle partijen bieden naast de kernfunctionaliteiten aanvullende diensten aan, zoals incident response, digital forensics, threat hunting, vulnerability management en ondersteuning bij compliance- en weerbaarheidsvraagstukken. Deze diensten worden veelal gepositioneerd als onderdeel van een bredere, risicogestuurde ontwikkeling van de cybersecurityvolwassenheid.

De borging van 24/7 dienstverlening wordt door partijen ingevuld met een combinatie van organisatorische maatregelen, technische redundantie en continuïteitsprocessen. Daarbij varieert de invulling van volledig bemande SOC-dienstverlening tot modellen waarbij buiten

kantooruren gebruik wordt gemaakt van geautomatiseerde detectie in combinatie met bereikbare specialisten.

Voor detectie en respons maken partijen gebruik van een combinatie van detectieregels, gedragsanalyse, threat intelligence en geautomatiseerde correlatie. MITRE ATT&CK wordt hierbij veelvuldig genoemd als uitgangspunt voor detectieontwikkeling. Meerdere partijen benadrukken dat de focus niet uitsluitend ligt op het genereren van meldingen, maar op het leveren van bruikbare analyses en handelingsperspectief.

Ten aanzien van risicogestuurd werken bestaat brede overeenstemming. Veelgenoemde frameworks zijn MITRE ATT&CK, NIST, ISO 27001, BIO en NIS2. Deze worden toegepast voor het bepalen van prioriteiten, het inrichten van detectie en het periodiek evalueren van risico's en dreigingen.

Alle partijen geven aan hybride IT-omgevingen integraal te kunnen monitoren. Voor OT-omgevingen bestaan aanvullende aandachtspunten, waaronder beperkte loggingmogelijkheden, beschikbaarheidseisen en afhankelijkheden van leveranciers. Meerdere partijen adviseren OT-monitoring gefaseerd te benaderen en afzonderlijk te beoordelen binnen de totale scope van de dienstverlening.

Over prestatie-indicatoren bestaat eveneens een grote mate van overeenstemming. Veelgenoemde KPI's hebben betrekking op detectie-, reactie- en hersteltijden, de kwaliteit van meldingen en de betrouwbaarheid van de dienstverlening. Daarnaast wijzen meerdere partijen op het belang van indicatoren die inzicht geven in risicoreductie, detectiedekking en de ontwikkeling van de cyberweerbaarheid van de organisatie.

Thema 3. Techniek en Architectuur (verkennend)

De marktpartijen beschrijven een duidelijke ontwikkeling van traditionele SIEM-oplossingen naar geïntegreerde securityplatformen waarin detectie, monitoring, respons en automatisering samenkomen. Daarbij worden SIEM-, XDR-, SOAR- en threat intelligence-functionaliteiten veelal in samenhang toegepast. Meerdere partijen adviseren een gefaseerde implementatie, waarbij wordt gestart met de meest kritieke onderdelen van de omgeving en vervolgens wordt uitgebreid op basis van risico's en prioriteiten.

Voor netwerkmonitoring onderscheiden partijen verschillende technische benaderingen. De meeste partijen adviseren een risicogestuurde aanpak waarbij bestaande logbronnen, netwerkinformatie en endpointdata gezamenlijk worden ingezet voor detectie en analyse. Voor specifieke omgevingen, zoals OT-netwerken of andere hoog-risico onderdelen van de infrastructuur, kunnen aanvullende detectiemogelijkheden worden ingezet.

Partijen zijn het erover eens dat moderne detectie niet uitsluitend kan steunen op traditionele detectieregels. Gedragsanalyse, threat intelligence, threat hunting en continue

doorontwikkeling van detectiemechanismen worden breed gezien als belangrijke onderdelen van een toekomstbestendige dienstverlening.

Ten aanzien van geautomatiseerde respons bestaat brede overeenstemming dat automatisering waardevol is, mits deze gecontroleerd en gefaseerd wordt toegepast. Meerdere partijen adviseren om impactvolle acties alleen uit te voeren binnen vooraf overeengekomen kaders en met passende menselijke controle. Voor OT-omgevingen wordt daarbij extra terughoudendheid aanbevolen.

Vrijwel alle partijen benadrukken het belang van data-eigenaarschap, open integratiemogelijkheden en het voorkomen van onnodige afhankelijkheden van leveranciers. Daarbij wordt aandacht gevraagd voor exporteerbaarheid van data, toepassing van open standaarden en duidelijke afspraken over beëindiging en overdracht van dienstverlening. Meerdere partijen noemen vendor lock-in expliciet als aandachtspunt en adviseren een modulaire architectuur waarbij componenten, data en processen zoveel mogelijk onafhankelijk van specifieke leveranciers kunnen functioneren. Daarnaast wijzen verschillende partijen op het belang van digitale soevereiniteit en transparantie binnen de keten van technologie en dienstverlening.

Transparantie over detectiedekking, resterende risico's en verbeterpunten wordt door veel partijen als belangrijk uitgangspunt genoemd. Daarbij wordt regelmatig verwezen naar MITRE ATT&CK als hulpmiddel om inzicht te geven in gedetecteerde aanvalstechnieken, de mate van detectiedekking en eventuele blinde vlekken. Het periodiek inzichtelijk maken van deze informatie wordt door meerdere partijen gezien als belangrijk instrument voor de verdere ontwikkeling en verbetering van de dienstverlening.

Thema 4. Werking van de SOC-dienstverlening

De meeste marktpartijen bieden een 24/7 SOC-dienstverlening aan met continue monitoring en incidentopvolging. Daarbij worden verschillende organisatiemodellen gehanteerd, variërend van permanent bemande SOC's tot hybride modellen waarin geautomatiseerde monitoring wordt gecombineerd met beschikbaarheidsdiensten buiten kantooruren.

Over de communicatie rondom incidenten bestaat grote overeenstemming. Partijen beschrijven een werkwijze waarbij incidenten via vooraf overeengekomen escalatieprocedures worden gecommuniceerd, ondersteund door rapportages, dashboards en periodieke evaluaties. Meerdere partijen geven aan ondersteuning te bieden bij wettelijke meld- en informatieverplichtingen.

De marktpartijen zien incidentafhandeling als een gezamenlijke verantwoordelijkheid tussen opdrachtgever en dienstverlener. Daarbij wordt verwacht dat de opdrachtgever betrokken blijft bij besluitvorming rondom risico's, prioriteiten en impactvolle

responsmaatregelen. Tevens wordt het belang benadrukt van actuele informatie over de IT- en OT-omgeving en duidelijke contact- en escalatiestructuren.

Voor de continuïteit van de dienstverlening maken partijen gebruik van organisatorische, technische en procesmatige maatregelen. Veelgenoemde voorzieningen zijn redundante SOC-omgevingen, uitwijkmogelijkheden, gestandaardiseerde processen en periodieke toetsing van continuïteitsmaatregelen. Daarnaast wijzen meerdere partijen op het belang van alternatieve communicatiemiddelen voor situaties waarin reguliere communicatiemiddelen niet beschikbaar zijn.

Ten aanzien van geautomatiseerde en mitigerende maatregelen bestaat brede overeenstemming dat deze waardevol kunnen zijn, mits verantwoordelijkheden, bevoegdheden en escalatieprocedures vooraf duidelijk zijn vastgelegd. Voor OT-omgevingen wordt daarbij extra terughoudendheid aanbevolen vanwege de mogelijke impact op operationele processen.

De samenwerking met bestaande IT- en OT-leveranciers wordt door partijen gezien als een belangrijk onderdeel van de dienstverlening. Daarbij worden duidelijke afspraken over rollen, verantwoordelijkheden, escalatieprocedures en wijzigingsbeheer als belangrijke randvoorwaarden genoemd.

Thema 5. Specificatie, Innovatie en Marktontwikkelingen

Vrijwel alle marktpartijen adviseren om de dienstverlening primair functioneel uit te vragen en technische eisen te beperken tot noodzakelijke randvoorwaarden. Volgens de markt biedt deze aanpak ruimte voor innovatie, sluit deze beter aan bij technologische ontwikkelingen en wordt onnodige afhankelijkheid van specifieke leveranciers voorkomen. Veelgenoemde randvoorwaarden zijn onder andere relevante certificeringen, naleving van wet- en regelgeving, ondersteuning van open standaarden en mogelijkheden voor data-export en overdracht.

Ten aanzien van marktontwikkelingen noemen partijen onder meer de toenemende toepassing van automatisering en AI binnen securityoperaties, de verdere integratie van detectie- en responsfunctionaliteiten en de groeiende aandacht voor identiteitsbeveiliging, OT-security en digitale soevereiniteit. Daarbij wordt benadrukt dat technologische ontwikkelingen ondersteuning bieden aan de dienstverlening, maar menselijke expertise en besluitvorming een belangrijk onderdeel blijven van effectieve cybersecurity.

De marktpartijen geven aan dat continue doorontwikkeling van de dienstverlening noodzakelijk is om aansluiting te houden bij veranderende dreigingen, technologieën en wet- en regelgeving. Veelgenoemde instrumenten zijn het periodiek actualiseren van detectieregels en use cases, het verwerken van lessons learned uit incidenten, het volgen

van relevante wet- en regelgeving en het structureel evalueren en verbeteren van de dienstverlening in samenwerking met de opdrachtgever.

Thema 6. Kosten en Contract

De marktpartijen adviseren om de prijsopbouw van de dienstverlening transparant en vergelijkbaar vorm te geven. Daarbij wordt veelal onderscheid gemaakt tussen eenmalige implementatiekosten, periodieke kosten voor de reguliere dienstverlening en variabele kosten die afhankelijk zijn van de omvang of complexiteit van de omgeving. Aanvullende diensten, zoals incident response, forensisch onderzoek of specialistische ondersteuning, worden doorgaans afzonderlijk geprijsd.

Voor een goede vergelijkbaarheid van inschrijvingen achten partijen het belangrijk dat alle inschrijvers uitgaan van dezelfde uitgangspunten en scope. Daarbij wordt aandacht gevraagd voor transparantie in de gehanteerde prijscomponenten en de factoren die van invloed zijn op de totale kosten gedurende de looptijd van de overeenkomst.

Thema 7. Overig

De marktpartijen noemen verschillende aandachtspunten voor de verdere uitwerking van de aanbesteding. Veelgenoemd zijn duidelijke afspraken over governance, verantwoordelijkheden, escalatieprocedures en het mandaat voor responsmaatregelen. Daarbij wordt benadrukt dat de dienstverlening niet alleen moet voorzien in signalering, maar ook in bruikbare opvolging en handelingsperspectief.

Daarnaast vragen meerdere partijen aandacht voor een realistische en gefaseerde scope. Met name OT-monitoring, datakwaliteit, volledigheid van logbronnen en retentietijden worden genoemd als onderwerpen die zorgvuldig moeten worden afgebakend. Een te brede initiële scope kan volgens partijen leiden tot hogere complexiteit, hogere kosten en een langere implementatieduur.

Tot slot worden digitale soevereiniteit, datalocatie, exit afspraken en overdraagbaarheid van data en documentatie genoemd als belangrijke aandachtspunten. Meerdere partijen adviseren om deze onderwerpen vooraf duidelijk te regelen, zodat continuïteit en beheersbaarheid gedurende en na afloop van de dienstverlening worden geborgd.