

Marktconsultatie SOC Dienstverlening

PCM00015 Marktconsultatie Format

Versie nummer: V1.0	Versie datum: 13-02-2023	Documentnummer: I&OSOC1
-------------------------------	------------------------------------	-----------------------------------

Auteur:	<i>ProRail</i>
Proceseigenaar:	<i>ICT I&O</i>
Status:	<i>Definitief</i>

Marktconsultatie

SOC Dienstverlening



Versie	1.0 (definitief)
Datum	16-02-2023
Status	Definitief
TN kenmerk	399482

ProRail

1	Algemeen	4
2	Procedure van de marktconsultatie	9
3	Communicatie / inlichtingen	11
4	Algemeen	13
5	Vragenlijsten	14

1 Algemeen

ProRail heeft grote ambities op het gebied van de (cyber) security van haar ICT-infrastructuur. Om deze ambities te realiseren is een Security Operations Center (SOC) naar de mening van ProRail essentieel. Om het huidige ProRail-SOC naar een hoger niveau te brengen wil ProRail graag met de markt overleggen over de dienstverleningsmogelijkheden die de markt op dit terrein kan bieden. Mogelijk leidt het traject naar een aanbesteding in welke vorm dan ook.

Een marktconsultatie is nog geen formeel onderdeel van een eventueel aanbestedingsproces. De marktconsultatie en daaruit verkregen antwoorden kunnen wel belangrijke input vormen in de keuze óf een aanbestedingsprocedure gestart wordt. Ook draagt het bij aan het opstellen van een duidelijke vraagstelling in een eventueel aanbestedingsdocument.

Wij stellen uw deelname op prijs, echter bent u niet verplicht uw medewerking te verlenen of (alle) vragen te beantwoorden. De marktconsultatie is voor betrokkenen vrijblijvend.

1.1 De vragende organisatie

Deze marktconsultatie wordt georganiseerd door ProRail B.V., hierna te noemen ProRail. ProRail is spoorwegbeheerder van Nederland en verantwoordelijk voor het gehele spoorwegnet.

Het KvK-nummer van ProRail B.V. is 30124359.

1.2 Over ProRail

ProRail is verantwoordelijk voor het spoorwegnet van Nederland: aanleg, onderhoud, beheer en veiligheid. Medewerkers zorgen ervoor dat elke dag, 24/7, 1.200.000 reizigers en 100.000 ton goederen op hun plaats van bestemming komen, met 6550 treinen over ruim 7000 kilometer spoor. Dit doet ProRail met aandacht voor de samenleving én met oog voor de toekomst.

ProRail staat voor duurzame mobiliteit. Door middel van innovatie maakt ProRail mogelijk dat er meer mensen met de trein kunnen reizen en meer goederen over het spoor vervoerd kunnen worden.

Het spoorwegnet is met recht het kloppend hart van mobiel Nederland. ProRail werkt aan de bereikbaarheid van Nederland door te zorgen voor een optimaal spoornetwerk. Denk aan: het verdelen van de capaciteit op het spoor, het regelen van alle treinverkeer, het bouwen en beheren van stations en het aanleggen van nieuw spoor. Tevens onderhoudt ProRail bestaande infrastructuur zoals spoor, wissels, seinen en overwegen. Voor meer informatie over de organisatie zie <https://www.prorail.nl/>.

1.3 Definitie SOC ProRail

1.3.1 Doelstelling

Het SOC is het organisatieonderdeel van ProRail dat specifiek is gericht op het vroegtijdig signaleren en voorkomen van cybersecurityincidenten.

1.3.2 Visie en doelstelling

ProRail wil zo cyber-secure zijn als ze maar kan zijn. Hierbinnen is het SOC gericht op het vroegtijdig signaleren, reageren op en voorkomen van cybersecurityincidenten.

Het ProRail SOC is het geheel van ProRail en externe partners dat bij concrete dreigingen hét expert-team, vormt, dat is gericht op het adviseren van mitigerende maatregelen om de gevolgen van cybersecurity incidenten te beperken en zo snel mogelijk tot functieherstel te komen van de bedrijfsvoering. Het SOC activeert de interne regievoering richting verschillende beheerteams tijdens incidenten, calamiteiten en in crisissituaties.

1.3.3 Strategie

Het ProRail SOC streeft de volgende strategische doelen na:

- Het signaleren, monitoren en opsporen van kwetsbaarheden en het coördineren (regie) en laten afhandelen van security-incidenten in de operationele infrastructuur (IT en OT) en applicaties.
- Het duiden van IT/OT security dreigingen.
- Het adviseren van mitigerende maatregelen t.a.v. de IT/OT security dreigingen (preventief) binnen de vastgestelde IT/OT security normen en kaders van ProRail.

1.4 Doelen van de marktconsultatie

Doelen van deze marktconsultatie zijn:

- a) Het verkrijgen van inlichtingen over de mogelijkheden van de markt(partijen) op het gebied van SOC-dienstverlening, inclusief de in de markt verkrijgbare oplossingen;
- b) Inzicht krijgen in welke SOC-gerelateerde activiteiten ProRail zelf intern wil blijven uitvoeren, welke activiteiten zullen worden aanbesteed en welke verantwoordelijkheid leveranciers bereid zijn daarin te nemen;
- c) Daarnaast willen wij inzicht ontwikkelen in de mogelijke samenwerkingsscenario's tussen ProRail en de leverancier en in de zaken die ProRail moet inrichten om goed met de leverancier te kunnen samenwerken;
- d) Inzicht te krijgen in de SOC-dienstverlening rondom een hybride omgeving (bestaande uit IT, OT, Cloud, KA);
- e) Inzicht te krijgen in de mate van standaardisatie in de SOC-markt;
- f) Inzicht te krijgen in de ervaring van marktpartijen met het aanbieden van SOC-diensten aan afnemers in de spoorsector en andere Aanbieders van Essentiële Diensten (AED's);
- g) Inzicht te krijgen in het aantal geïnteresseerde marktpartijen;
- h) Te weten komen welke informatie marktpartijen minimaal nodig hebben om een goed voorstel te kunnen doen;
- i) Inzicht krijgen in de innovaties die momenteel gaande zijn in de SOC-markt;
- j) Inzicht te krijgen in de voordelen en business cases die horen bij deze innovaties;
- k) Inzicht te krijgen in de verschillende soorten SOC-leveranciers, het soort partij ProRail zou moeten zoeken en welke relatie er moet worden aangegaan.

1.5 De huidige situatie

Het proces 'vervoer van personen en goederen over (hoofd)spoorweginfrastructuur' is door het Rijk aangewezen als vitaal proces (categorie B) en daarmee onderdeel geworden van de Nederlandse vitale

infrastructuur. Dit brengt nieuwe aspecten en wettelijke verplichtingen omtrent IT (cyber)security met zich mee. Hier speelt een doorontwikkeling van het SOC een substantiële rol in. Daarnaast laten het Dreigingsbeeld Spoor en het jaarlijkse Cybersecuritybeeld van het NCSC zien dat digitale dreigingen sterk aan het toenemen zijn. ProRail beschikt over een SOC dat op basis van een Security Information & Event Management (SIEM) geaggregeerd en gecorreleerde log- en netwerkgegevens analyseert en indien nodig rapporteert.

1.5.1 SOC-team

ProRail beschikt over een virtueel SOC-team. De leden zijn medewerkers uit de lijn aangevuld met een aantal externe cybersecurityspecialisten. Het SOC-team maakt gebruik van een beperkt contract van een SOC-dienstverlener. De gewenste focus van ProRail is het beperken van de impact op de treindienst. Daarnaast ligt de focus ook op 24/7 monitoring van het gehele ICT-landschap, met als doel om (security)incidenten te voorkomen. Waarbij er gebruikt wordt gemaakt van de kracht van de markt (kennis en ervaringen) om te komen tot het beste resultaat - zo snel mogelijk tot functieherstel te komen van de bedrijfsvoering.

Het SOC-team is ontstaan vanuit een behoefte. Onderdeel van de marktconsultatie is ook te onderzoeken wat ProRail intern moet gaan inregelen om een goede aansluiting te krijgen op de nieuwe SOC-dienstverlener.

1.5.2 Incidentproces

ProRail beschikt over een goed werkend incidentproces. Incidenten (ook security incidenten) worden gemeld via het standaard incidentenproces bij de Centrale Servicedesk (CSD). ProRail heeft met twee externe partijen een rechtstreekse relatie met betrekking tot security events.

1.5.3 Datacenters en infrastructuur

ProRail beschikt over redundante on-premise datacenters en cloud oplossingen (Azure).

Aandachtspunten:

- a) ProRail heeft een landelijke infrastructuur. Het beheer van de ICT-infrastructuur is niet uitbesteed.
- b) Deze landelijke infrastructuur is op ongeveer 1.100 locaties in het land beschikbaar.
- c) Veel van deze locaties hebben alleen ongeconditioneerde behuizingen.
- d) Voor het koppelen van deze onderposten wordt in de infrastructuur gebruik gemaakt van het cascaderen van locaties.
- e) Er is geen centrale locatie aanwezig waar al deze verkeerstromen langskomen. Er is een asynchrone communicatie.

1.5.4 Security monitoring

Op dit moment besteedt ProRail een deel van de monitoring uit. Op verschillende domeinen wordt security logging gedaan door verschillende partijen. Dit betreft in het bijzonder Security Monitoring op de gehele KA-omgeving. Een andere partij monitort ook nog een beperkt aantal systemen, zoals de AD-omgeving. ProRail heeft zelf een Splunk-omgeving, maar dit is alleen voor de netwerkomgeving en het verkeersleidingdomein (waarin de treinenloop wordt bestuurd) - nog niet de KA en OT. Een andere onderaannemer logt en monitort de OT-omgeving.

Daarnaast zijn er ook domeinen waar geen security logging is ingericht.

1.5.5 Applicatielandschap

ProRail maakt gebruik van zowel on premise als van IAAS/PAAS/SAAS-applicaties. Beide modaliteiten vallen binnen de scope van deze marktconsultatie. Een aantal applicaties bij ProRail zijn vitaal. Bij uitval van deze applicaties kan bijvoorbeeld de treindienst aangetast worden. De applicaties/toepassingen die gedefinieerd zijn als bedrijfskritisch /vitaal vallen binnen het BCM (Business Continuity Management) van ProRail.

1.6 Beoogde scope

ProRail heeft nog niet besloten welke dienstverlening uit te besteden aan een leverancier. De scope van de uitgevraagde diensten zal in ieder geval zowel de IT als de OT omvatten.

Voorbeelden van diensten die ProRail zou kunnen aanbesteden zijn (geen uitputtende lijst):

- a) Security monitoring;
- b) Intrusion Detection & Prevention;
- c) Security Analysis;
- d) Threat Intelligence;
- e) Forensisch onderzoek;
- f) Incident management systeemkoppeling;
- g) Threat Hunting.

a)

1.7 De gewenste situatie

ProRail wil graag haar huidige SOC-dienst vervangen door een nieuwe dienst met een bredere scope: aangeduid als SOC 2.0. Hierbij gaat de voorkeur van ProRail uit naar gespecialiseerde cybersecurity dienstverleners.

1.7.1 Leidende principes

Het nieuwe SOC moet worden ingericht conform de volgende leidende principes:

1. De gespecialiseerde markt kent de huidige mogelijkheden en beperkingen van SOC-diensten het beste;
2. ProRail werkt als regie-organisatie en besteedt zoveel mogelijk gespecialiseerde SOC-diensten uit met uitzondering van de ICT-operatie;
3. ProRail maakt gebruik van derde partijen om haar SOC, fysiek en virtueel optimaal te kunnen benutten;
4. ProRail blijft te allen tijde eigenaar van haar log- en monitoring data en slaat deze het liefst in een door ProRail beheerde omgeving op.
5. ProRail en al haar contractpartijen werken en hebben kennis van de BIO, de IEC62443 en CenelecTS50701;
6. ProRail en haar dienstverlener werken samen met de SOC's van de ketenpartners en het ministerie;
7. ProRail werkt samen met haar stakeholders aan de cyberveiligheid.

Voor bepaalde informatiebeveiligingsdiensten wenst ProRail dat deze dienstverlening 24 x 7 plaatsvindt. Echter, beschikt ProRail niet over de resources om deze beschikbaarheid van diensten te leveren.

Van de aanbieder van het SOC wordt verwacht dat hij de beschikking heeft over een modern SIEM dat vanuit de ProRail-logbronnen kan worden gevoed. Ook wil ProRail geïnformeerd worden over de 'best practices' met betrekking tot sensoren in haar omgeving.

2 Procedure van de marktconsultatie

2.1 Openbare marktconsultatie

Deze marktconsultatie is gepubliceerd op TenderNed als open marktconsultatie. Dit houdt in dat alle partijen in de markt de gelegenheid krijgen deel te nemen. Iedere onderneming die in staat is de door ProRail gestelde vragen zoals aangegeven in hoofdstuk 5 te beantwoorden, mag deelnemen aan deze marktconsultatie.

Partijen worden gevraagd schriftelijk te reageren op de gestelde vragen. ProRail kan ervoor kiezen om een of meerdere partijen uit te nodigen voor een nadere mondelinge toelichting op de gegeven antwoorden.

2.2 Planning

Hieronder is een *indicatieve* planning aangegeven voor het verloop van deze procedure.

Datum	Activiteit
Donderdag 16 februari	Publicatie Marktconsultatie
Maandag 27 februari	Sluitingstermijn voor het stellen van vragen over de Leidraad
Maandag 6 maart	Verstrekken van antwoorden op de gestelde vragen en evt. gewijzigde documentatie door ProRail (Publicatie van Nota van Inlichtingen).
Maandag 20 maart	Uiterste datum voor het indienen van de antwoorden op de vragen in hoofdstuk 5.
Donderdag 6 april	Individuele gesprekken.
Vrijdag 14 april	Concept verslag individuele gesprekken (ter controle en voor akkoord versturen naar de individuele deelnemers marktconsultatie)
Vrijdag 21 april	Vaststelling individuele gesprekken
Maandag 24 april	Concept verslag marktconsultatie versturen naar deelnemers marktconsultatie
Maandag 1 mei	Vaststelling verslag marktconsultatie
Dinsdag 2 mei	Publiceren eindverslag marktconsultatie op TenderNed .

Belangstellenden kunnen aan deze planning geen rechten ontlelen. ProRail behoudt zich te allen tijde het recht voor om de planning te wijzigen.

2.3 Voorbehouden

Deelnemen aan de marktconsultatie is geheel vrijwillig en zal niet leiden tot enige voorrechten in een aanbesteding. Evenzo zal niet deelnemen in de marktconsultatie niet leiden tot uitsluiting van een eventuele aanbesteding.

Door uw deelname aan deze marktconsultatie stemt u er mee in dat de door u verstrekte informatie door ProRail mag worden gebruikt in (de voorbereiding van) de eventuele aanbesteding. Door u verstrekte commerciële (cijfermatige) informatie zal door ProRail vertrouwelijk worden behandeld. Door u aan te geven welke informatie commercieel betreft. Marktpartij dient eveneens vertrouwelijk om te gaan met de door ProRail verstrekte informatie gedurende het proces.

Marktpartij zal zich onthouden van gedragingen die de mededinging tussen marktpartijen beperken. In het bijzonder zal marktpartij:

- a) ProRail niet belemmeren in zijn streven met een andere marktpartij of een derde tot overeenstemming te komen;
- b) Geen informatie over zijn beantwoording marktconsultatie uitwisselen met andere marktpartijen.

Eventuele kosten voor de deelname aan deze marktconsultatie worden niet vergoed.

2.4 Publicatie

Wanneer in vervolg op de marktconsultatie door ProRail een aanbesteding wordt uitgevoerd, wordt door ProRail een beknopte geanonimiseerde samenvatting van de marktconsultatie bij de aanbestedingsstukken gepubliceerd.

3 Communicatie / inlichtingen

3.1 TenderNed

Alle communicatie bij de marktconsultatie verloopt via TenderNed. Vanzelfsprekend is het van belang dat Deelnemers op de hoogte zijn van de functionaliteiten van TenderNed en dat het goed functioneert binnen de eigen ICT-omgeving. Voor alle technische vragen m.b.t. TenderNed dient men zich te wenden tot de helpdesk van TenderNed.

3.2 Contact

ProRail werkt bij deze marktconsultatie met een vaste contactpersoon. Alle contacten met ProRail betreffende de marktconsultatie verlopen via deze contactpersoon. Het is Deelnemers nadrukkelijk niet toegestaan om zonder instemming van ProRail contact te zoeken of te onderhouden met andere medewerkers, adviseurs of klanten van ProRail met betrekking tot de marktconsultatie, behalve door ProRail georganiseerde inlichtingenbijeenkomst(en) en gesprekken. Overtreding van deze regel kan leiden tot uitsluiting van deelname aan de procedure.

Voor vragen over en aanmelden voor deze marktconsultatie kunt contact opnemen met:
Bob Snelle (Tendermanager ProRail)
06 28 59 57 98

In beginsel zal de procedure volledig via TenderNed worden uitgevoerd. Voor het geval dat toch rechtstreeks contact noodzakelijk is, wenst ProRail de contactgegevens te ontvangen van een contactpersoon van de Deelnemer.

Voor het contact met ProRail dient marktpartij één contactpersoon en één plaatsvervanger aan te wijzen, die beiden bij marktpartij in dienst zijn. Marktpartij vermeldt de naam, functie en adresgegevens van deze contactpersonen die op verzoek van ProRail een toelichting op de Beantwoording Marktconsultatie kunnen verschaffen.

3.3 Vragen over de leidraad

Geïnteresseerden kunnen vragen stellen over de Leidraad. Die vragen en/of opmerkingen over de Leidraad dienen uiterlijk op de in de planning aangegeven datum en tijd via TenderNed te worden gestuurd naar de Contactpersoon.

De vragen zullen geanonimiseerd worden beantwoord in een Nota van Inlichtingen.

3.4 Individuele gesprekken

Na ontvangst van de door Deelnemers ingevulde vragenlijst bestaat de mogelijkheid dat ProRail met een of meerdere geïnteresseerde partijen individuele gesprekken voert, om de vragen en antwoorden te bespreken en nader toe te lichten. Voorafgaan aan het gesprek ontvangt de Deelnemer een agenda.

Om het gesprek efficiënt te kunnen laten verlopen stellen wij het op prijs wanneer u met maximaal drie personen aanwezig bent.

Van de individuele gesprekken wordt een verslag gemaakt. Dit verslag is niet openbaar. Wel kan ProRail informatie uit het verslag gebruiken bij het opstellen van het eindverslag van de marktconsultatie.

Indien u wordt uitgenodigd voor een toelichtingssessie, wordt in overleg met u een passend tijdstip gepland voor donderdag 6 april. Duur van de sessie bedraagt circa 1,5 uur.

4 Algemeen

4.1 Procedure

Bij afronding van de marktconsultatie, organiseert ProRail een aanbesteding voor de gunning van een opdracht, die mede gedefinieerd zal worden op basis van de resultaten van de marktconsultatie.

4.2 Aanbiedingsbrief

De Deelnemer mag een aanbiedingsbrief indienen waarin een toelichting wordt gegeven op de ingevulde vragenlijst. Indienen van een aanbiedingsbrief is niet verplicht

4.3 Vertrouwelijkheid

Door deel te nemen aan deze marktconsultatie stemt de Deelnemer er mee in dat de door hem verstrekte informatie, anoniem, door ProRail mag worden gebruikt in (de voorbereiding) van een eventuele aanbesteding.

Eventuele verstrekte commercieel vertrouwelijke (prijs)informatie zal door ProRail vertrouwelijk worden behandeld.

Een Deelnemer kan aan ProRail verzoeken vóór verstrekking van bepaalde gevoelige informatie om deze informatie geheim te houden. ProRail kan hiermee instemmen.

4.4 Intellectuele eigendom

Behoudens uitzonderingen door de wet gesteld mag zonder schriftelijke toestemming van ProRail niets uit deze Leidraad of de bijlagen worden verveelvoudigd (anders dan voor het doel van deze Leidraad) door middel van druk, fotokopie, microfilm, of anderszins. Dit is zowel van toepassing op de volledige documenten als op delen ervan.

4.5 Voorbehouden opdrachtgever

Uit deze Leidraad vloeien geen verplichtingen voort voor ProRail anders dan de verplichting zich aan de eigen procedureregels en de wettelijke regels te houden. ProRail behoudt zich het recht voor om in elk stadium de procedure op te schorten en/of definitief te staken.

In geen enkel geval kan er sprake zijn van enige verplichting van ProRail tot vergoeding van welke schade of kosten dan ook.

4.6 Merken, octrooien en dergelijke

Overall waar in de Leidraad of bijlagen wordt verwezen naar een fabricaat, een bepaalde herkomst of een bijzonder werkwijze, een merk, keurmerk of certificaat betreffende duurzaamheid, milieu of dierenwelzijn, dan wel gebaseerd op sociale overwegingen, een octrooi of een type, een bepaalde oorsprong of een bepaalde productie dient te worden gelezen "of gelijkwaardig".

5

Vragenlijsten

Zie bijlage 2 vragenlijst