1. Koper

1.1 Koper

Officiële naam:	Kamer van Koophandel
Rechtsvorm van de koper:	Publiekrechtelijke instelling
Activiteit van de aanbestedende dienst:	Algemene overheidsdiensten

2. Procedure

2.1 Procedure

Titel:	SOC Analist 2x
Beschrijving:	Binnen de Kamer van Koophandel is er een product genaamd Cyber Security Operations. Het team draagt zorg voor de gehele bedrijfsvoering van de veiligheid over de deelgebieden bescherming, verdediging, weerbaarheid en governance. Dit doen we door verschillende clusters in het productteam onder te brengen met 1 gezamenlijk doel; de KVK een veiligere plek maken. De ontwikkelingen rondom het onderwerp security gaan steeds sneller en is een belangrijk thema in de bedrijfsvoering. Het productteam wil daardoor de reeds gemaakte roadmap en de vernieuwde strategie verder gaan uitvoeren. Het productteam werkt in scrum teams aan ontwikkeling en beheer. De teams zijn breed en multidisciplinair samen gesteld. Voor het maken van de volgende stap voor het productteam is de KVK op zoek naar twee Cybersecurity SOC analisten.De SOC analist maakt deel uit van het Security Operations Center (SOC). Als SOC analist monitor je de cybersecurity status van de organisatie, handel je incidenten als gevolg van cybersecurity aanvallen en draag je zorg voor de beschikbaarheid en continu?teit van de KVK dienst verlening.De kandidaat werkt aan het pro- en reactief aan het bewaken en onderhouden van de cybersecurity weerbaarheid van KVK. Hieraan valt te denken: - Reguliere monitoring en analyse security-incidenten volgens afgesproken kaders; - Stem af met de diverse oplosgroepen en neemt de regie bij het tijdig oplossen van security incidenten; - Documenteren incident resultaten en uitgevoerde handelingen; - Ontwikkelen, onderhouden en validateren van het Incident Response Plan; - Bijdrage leveren aan het verbeteren en valideren van het incident afhandeling proces; - Periodiek uitvoeren van een kwetsbaarheden onderzoek naar bedreigingen volgens afgesproken kaders en indien nodig n.a.v. penetratietesten; - Bepaal je in samenspraak met ontwikkelteams de inhoud en diepgang van penetratietesten; - Voer je periodieke rapportages uit over de operationele security resultaten en draagt zorg voor de verbeter activiteiten; - Meten van effectiviteit detectie incidenten en response; - Analyseren en beoordelen cybersecurity controls en mitigatie acties na een incident; - Ontwikkelen en invoeren test methoden op het incident afhandeling; - Analyseren en onderzoeken vraagstukken op het gebied van IT-security; - Voer je periodieke beoordelingsanalyse uit op de geleverde producten en diensten; - Stel risicoclassificaties op binnen verschillende IT-security gebieden; - Geef gevraagd en ongevraagd adviezen over IT-security vraagstukken; - Maken, onderhouden en valideren van use cases; - Maken, onderhouden en valideren van play books; - Samenwerken met het Cyber Security Incident Response Team (CSIRT). De kandidaat werkt samen met de product owner en het product team. Hierbij is de kandidaat gewend om te werken binnen de kaders en richtlijnen van een bestaande security architectuur en informatie beveiliging normen, standaarden en frameworks. (bv ISO, NIST, Mitre etc.) Vanuit de werkzaamheden opereert de kandidaat als een teamplayer maar ook zelfstandig waarbij zowel mondeling als in schrift goed wordt gecommuniceerd /rapporteert. Van de kandidaat wordt verwacht dat hij/zij kritisch meedenkt inzake het verbetering van detectie, monitoring en response met als doel het verbeteren van de cybersecurity van de KVK.
Identificatiecode van de procedure:	6c9fb434-c908-4d3b-9b98-7591f8872be0
Interne identificatiecode:	1252
Type procedure:	Openbaar

Binnen de Kamer van Koophandel is er een product genaamd Cyber Security Operations. Het team draagt zorg voor de gehele bedrijfsvoering van de veiligheid over de deelgebieden bescherming, verdediging, weerbaarheid en governance. Dit doen we door verschillende clusters in het

Rijksoverheid

Belangrijkste kenmerken van de procedure:	productteam onder te brengen met 1 gezamenlijk doel; de KVK een veiligere plek maken. De ontwikkelingen rondom het onderwerp security gaan steeds sneller en is een belangrijk thema in de bedrijfsvoering. Het productteam wil daardoor de reeds gemaakte roadmap en de vernieuwde strategie verder gaan uitvoeren. Het productteam werkt in scrum teams aan ontwikkeling en beheer. De teams zijn breed en multidisciplinair samen gesteld. Voor het maken van de volgende stap voor het productteam is de KVK op zoek naar twee Cybersecurity SOC analisten.De SOC analist maakt deel uit van het Security Operations Center (SOC). Als SOC analist monitor je de cybersecurity status van de organisatie, handel je incidenten als gevolg van cybersecurity aanvallen en draag je zorg voor de beschikbaarheid en continu?teit van de KVK dienst verlening.De kandidaat werkt aan het pro- en reactief aan het bewaken en onderhouden van de cybersecurity weerbaarheid van KVK. Hieraan valt te denken: - Reguliere monitoring en analyse security-incidenten volgens afgesproken kaders; - Stem af met de diverse oplosgroepen en neemt de regie bij het tijdig oplossen van security incidenten; - Documenteren incident resultaten en uitgevoerde handelingen; - Ontwikkelen, onderhouden en validateren van het Incident Response Plan; - Bijdrage leveren aan het verbeteren en valideren van het incident afhandeling proces; - Periodiek uitvoeren van een kwetsbaarheden onderzoek naar bedreigingen volgens afgesproken kaders en indien nodig n.a.v. penetratietesten; - Bepaal je in samenspraak met ontwikkelteams de inhoud en diepgang van penetratietesten; - Voer je periodieke rapportages uit over de operationele security resultaten en draagt zorg voor de verbeter activiteiten; - Meten van effectiviteit detectie incidenten en response; - Analyseren en beoordelen cybersecurity controls en mitigatie acties na een incident; - Ontwikkelen en invoeren test methoden op het incident afhandeling; - Analyseren en onderzoeken vraagstukken op het gebied van IT-security; - Voer je periodieke beoordelingsanalyse uit op de geleverde producten en diensten; - Stel risicoclassificaties op binnen verschillende IT-security gebieden; - Geef gevraagd en ongevraagd adviezen over IT-security vraagstukken; - Maken, onderhouden en valideren van use cases; - Maken, onderhouden en valideren van play books; - Samenwerken met het Cyber Security Incident Response Team (CSIRT). De kandidaat werkt samen met de product owner en het product team. Hierbij is de kandidaat gewend om te werken binnen de kaders en richtlijnen van een bestaande security architectuur en informatie beveiliging normen, standaarden en frameworks. (bv ISO, NIST, Mitre etc.) Vanuit de werkzaamheden opereert de kandidaat als een teamplayer maar ook zelfstandig waarbij zowel mondeling als in schrift goed wordt gecommuniceerd /rapporteert. Van de kandidaat wordt verwacht dat hij/zij kritisch meedenkt inzake het verbetering van detectie, monitoring en response met als doel het verbeteren van de cybersecurity van de KVK.

2.1.1 Doel

Aard van het contract :	Diensten
Belangrijkste classificatie (cpv):	79620000 Diensten voor de terbeschikkingstelling van personeel, met inbegrip van tijdelijk personeel

2.1.2 Plaats van uitvoering

Waar dan ook

2.1.4 Algemene informatie

Rechtsgrondslag:

Richtlijn 2014/24/EU

5. Perceel

5.1 Technische ID van het kavel: LOT-0001

Titel:	SOC Analist 2x
	Binnen de Kamer van Koophandel is er een product genaamd Cyber Security Operations. Het team draagt zorg voor de gehele bedrijfsvoering van de veiligheid over de deelgebieden bescherming, verdediging, weerbaarheid en governance. Dit doen we door verschillende clusters in het productteam onder te brengen met 1 gezamenlijk doel; de KVK een veiligere plek maken. De ontwikkelingen rondom het onderwerp security gaan steeds sneller en is een belangrijk thema in de bedrijfsvoering. Het productteam wil daardoor de reeds gemaakte roadmap en de vernieuwde strategie verder gaan uitvoeren. Het productteam werkt in scrum teams aan ontwikkeling en beheer. De teams zijn breed en multidisciplinair samen gesteld. Voor het maken van de volgende stap voor het productteam is de KVK op zoek naar twee Cybersecurity SOC analisten.De SOC analist

Rijksoverheid

Beschrijving:	maakt deel uit van het Security Operations Center (SOC). Als SOC analist monitor je de cybersecurity status van de organisatie, handel je incidenten als gevolg van cybersecurity aanvallen en draag je zorg voor de beschikbaarheid en continu?teit van de KVK dienst verlening.De kandidaat werkt aan het pro- en reactief aan het bewaken en onderhouden van de cybersecurity weerbaarheid van KVK. Hieraan valt te denken: - Reguliere monitoring en analyse security-incidenten volgens afgesproken kaders; - Stem af met de diverse oplosgroepen en neemt de regie bij het tijdig oplossen van security incidenten; - Documenteren incident resultaten en uitgevoerde handelingen; - Ontwikkelen, onderhouden en validateren van het Incident Response Plan; - Bijdrage leveren aan het verbeteren en valideren van het incident afhandeling proces; - Periodiek uitvoeren van een kwetsbaarheden onderzoek naar bedreigingen volgens afgesproken kaders en indien nodig n.a.v. penetratietesten; - Bepaal je in samenspraak met ontwikkelteams de inhoud en diepgang van penetratietesten; - Voer je periodieke rapportages uit over de operationele security resultaten en draagt zorg voor de verbeter activiteiten; - Meten van effectiviteit detectie incidenten en response; - Analyseren en beoordelen cybersecurity controls en mitigatie acties na een incident; - Ontwikkelen en invoeren test methoden op het incident afhandeling; - Analyseren en onderzoeken vraagstukken op het gebied van IT-security; - Voer je periodieke beoordelingsanalyse uit op de geleverde producten en diensten; - Stel risicoclassificaties op binnen verschillende IT-security gebieden; - Geef gevraagd en ongevraagd adviezen over IT-security vraagstukken; - Maken, onderhouden en valideren van use cases; - Maken, onderhouden en valideren van play books; - Samenwerken met het Cyber Security Incident Response Team (CSIRT). De kandidaat werkt samen met de product owner en het product team. Hierbij is de kandidaat gewend om te werken binnen de kaders en richtlijnen van een bestaande security architectuur en informatie beveiliging normen, standaarden en frameworks. (bv ISO, NIST, Mitre etc.) Vanuit de werkzaamheden opereert de kandidaat als een teamplayer maar ook zelfstandig waarbij zowel mondeling als in schrift goed wordt gecommuniceerd /rapporteert. Van de kandidaat wordt verwacht dat hij/zij kritisch meedenkt inzake het verbetering van detectie, monitoring en response met als doel het verbeteren van de cybersecurity van de KVK.
Interne identificatiecode:	1252

5.1.1 Doel

Aard van het contract :	Diensten
Belangrijkste classificatie (cpv):	79620000 Diensten voor de terbeschikkingstelling van personeel, met inbegrip van tijdelijk personeel

5.1.2 Plaats van uitvoering

Waar dan ook	
Aanvullende informatie:	

5.1.6 Algemene informatie

Aanbestedingsproject dat geheel of gedeeltelijk uit EU-fondsen wordt gefinancierd	
De aanbesteding valt onder de Overeenkomst inzake overheidsopdrachten (GPA):	ja

5.1.10 Gunningscriteria

Criterium:	
Type:	Prijs
Naam:	Prijsgedeelte
Beschrijving:	Prijsgedeelte. Weging: 30%.
Categorie van het gunningscriterium drempel:	Gewicht (percentage, exact)

Rijksoverheid

Gunningscriterium numerieke waarde:	30
Criterium:	
Type:	Kwaliteit
Naam:	Kwaliteitsgedeelte
Beschrijving:	Kwaliteitsgedeelte. Weging: 70%.
Categorie van het gunningscriterium drempel:	Gewicht (percentage, exact)
Gunningscriterium numerieke waarde:	70

5.1.15 Technieken

Raamovereenkomst:

Geen raamovereenkomst

Informatie over het dynamische aankoopsysteem:

Dynamisch aankoopsysteem, ook te gebruiken door niet in deze aankondiging vermelde kopers

Elektronische veiling: ja

5.1.16 Nadere inlichtingen, bemiddeling en evaluatie

Organisatie voor beroepsprocedures:	Kamer van Koophandel
Informatie over de termijnen voor beroep:	Beroep moet worden ingesteld binnen de toepasselijke wettelijke termijnen.

6. Resultaten

Waarde van alle contracten toegekend in deze kennisgeving:	89 Euro

6.1 ID resultaat perceel: LOT-0001

Er is ten minste één winnaar gekozen.

6.1.2 Informatie over winnaars

Winnaar:	
Officiële naam:	ResultaatGroep B.V.
Inschrijving:	
Identificatiecode van de inschrijving:	TENDER-1
Identificatiecode van het perceel of de groep percelen:	LOT-0001
Waarde van de aanbesteding:	89 Euro
Onderaanneming:	Neen

Informatie over het contract:

Identificatiecode van het contract:	CONTRACT-1
Datum waarop de winnaar is gekozen:	26/08/2026
Datum van sluiting van het contract:	26/08/2026

Rijksoverheid

6.1.4 Statistische informatie

Ontvangen inschrijvingen of verzoeken tot deelname:

Type van de ontvangen inschrijvingen:	Inschrijvingen
Aantal ontvangen inschrijvingen of verzoeken tot deelname:	1

8. Organisaties

8.1 ORG-0001

Officiële naam:	Kamer van Koophandel
Registratienummer:	59581883
Postadres:	St.-Jacobsstraat
Stad:	Utrecht
Postcode:	3511BT
Onderverdeling land (NUTS):	Alkmaar en omgeving (NL328)
Land:	Nederland
Contactpunt:	De heer Budgethouder KvK
E-mail:	recruitment@kvk.nl
Telefoon:	+31 885851585
Internetadres:	http://www.kvkhuurtin.nl
Kopersprofiel:	http://www.kvkhuurtin.nl

Rollen van deze organisatie:

Koper

Aankoopcentrale die overheidsopdrachten gunt of raamovereenkomsten sluit voor werken, leveringen of diensten die voor andere kopers bestemd zijn

8.1 ORG-0002

Officiële naam:	Kamer van Koophandel
Registratienummer:	59581883
Postadres:	St.-Jacobsstraat
Stad:	Utrecht
Postcode:	3511BT
Onderverdeling land (NUTS):	Alkmaar en omgeving (NL328)
Land:	Nederland
Contactpunt:	De heer / mevrouw Menno van der Meulen
E-mail:	recruitment@kvk.nl
Telefoon:	+31 885851585
Internetadres:	https://www.kvk.nl

Rollen van deze organisatie:

Organisatie voor beroepsprocedures

8.1 ORG-0003

Officiële naam:	ResultaatGroep B.V.
Omvang van de ondernemer:	Micro, klein of middelgroot

Rijksoverheid

Registratienummer:	54835658
Postadres:	Euclideslaan
Stad:	Utrecht
Postcode:	3584 BV
Onderverdeling land (NUTS):	Alkmaar en omgeving (NL328)
Land:	Nederland
Contactpunt:	De heer Jason Kartodimedjo
E-mail:	recruitment@resultaatgroep.nl
Telefoon:	+31 852015083
Rollen van deze organisatie:	
Inschrijver	
Winnaar van deze percelen:	LOT-0001

Informatie over een aankondiging

Identificatiecode /versie van de aankondiging:	233db241-95fa-45cc-80b2-6789d806b979 - 01
Type formulier:	Resultaat
Type aankondiging:	Aankondiging van een gegunde opdracht of concessie – standaardregeling
Verzenddatum van de aankondiging:	26/08/2026 05:00 +02:00
Talen waarin deze aankondiging officieel beschikbaar is:	Nederlands

Rijksoverheid