

Volgnr.	Ref.	Vraag	Antwoord
1	Scope	Kan Aanbestedende dienst aangeven wat de volledige scope inhoudt? Met de huidige informatie kan Gegadigde niet voldoende informatie achterhalen van het totale project.	Het IP aantal extern is ongeveer 50. Het IP aantal intern is ongeveer 1500 (loopt uiteen van servers, databases, switches, werkstations, accespoints, printers, etc.). Het IP aantal IoT is onbekend tot op heden.
2	Scope	Om voor de beoogde scope een gedegen prijsindicatie voor te stellen heeft Gegadigde informatie nodig over de hoeveelheid IP-adressen waarover de pentesten worden uitgevoerd. Kunt u deze aanleveren?	Het IP aantal extern is ongeveer 50. Het IP aantal intern is ongeveer 1500 (loopt uiteen van servers, databases, switches, werkstations, accespoints, printers, etc.). Het IP aantal IoT is onbekend tot op heden.
3	Bijlage 2, Nr. 2.	In de huidige eisen wordt het CCV-keurmerk voor penetratietesten niet gevraagd, terwijl dit in de markt als een belangrijk kwaliteitskenmerk wordt beschouwd voor dit type dienstverlening. Is opdrachtgever bereid dit keurmerk alsnog op te nemen als minimumeis en als onderdeel van de kwaliteitsbeoordeling, gezien het belang ervan voor het borgen van de kwaliteit van penetratietesten? Zo nee, licht toe.	Ja, het CCV-keurmerk wordt opgenomen als minimumeis.
4	Bijlage 2, Nr. 2.	De CREST certificatie wordt nauwelijks in Nederland toegepast en is aan een selectief kleine set van partijen verleend. Dit beperkt heel veel partijen om aan te bieden en bevoordeeld een klein, select aantal partijen. Wil Opdrachtgever deze eis laten vervallen? Zo nee, wat is de specifieke reden voor deze certificatie, ook in het licht van de CCV-keurmerk standaard binnen de pentestwereld?	Ja, de CREST-certificering vervalt.
5	Bijlage 2, Nr. 2.	Opdrachtnemer stelt voor om ook ISO9001, kwaliteitsmanagement toe te voegen, naast de ISO27001. Wil Opdrachtgever dit a.u.b. als eis toevoegen?	Nee, ISO27001 is voldoende.
6	Bijlage 2, Nr. 2.	Opdrachtnemer stelt voor om ook OSEP certificering mee te nemen als eis. Deze is heel gebruikelijk in de pentestwereld. Wil Opdrachtgever dit a.u.b. als eis toevoegen?	We nemen deze op in het voorbeeld lijstje van certificeringen, maar niet als eis.
7	Bijlage 2, Nr. 17	Opdrachtnemers missen informatie voor wat betreft de grootte en complexiteit van de omgeving om een accurate inschatting te maken voor de investering voor de pentest(en). Wij adviseren Opdrachtgever om meer informatie te delen over de grootte van de omgeving en de technische infrastructuur. Wil Oprachtgever a.u.b. aanvullende informatie verstrekken? Indien niet akkoord, wat is de reden hiervoor?	Het IP aantal extern is ongeveer 50. Het IP aantal intern is ongeveer 1500 (loopt uiteen van servers, databases, switches, werkstations, accespoints, printers, etc.). Het IP aantal IoT is onbekend tot op heden.
8	dCI-000492	Kunnen bedrijven die gevestigd zijn in Europa maar niet in Nederland deelnemen aan deze marktconsultatie en eventuele daaropvolgende aanbesteding?	Ja dat is mogelijk. De op te leveren rapporten dienen wel in het Nederlands te zijn opgesteld en daarnaast dient Nederlands de voertaal te zijn van de medewerkers die de opdracht uitvoeren bij de gemeente.
9	dCI-000492	Kunnen bedrijven met partners of onderaannemers in Europa, maar niet in Nederland deelnemen aan deze marktconsultatie en eventuele daaropvolgende aanbesteding?	Ja dat is mogelijk. De op te leveren rapporten dienen wel in het Nederlands te zijn opgesteld en daarnaast dient Nederlands de voertaal te zijn van de medewerkers die de opdracht uitvoeren bij de gemeente.
10	dCI-000492	Kunnen bedrijven met partners of onderaannemers buiten Europa deelnemen aan deze marktconsultatie en eventuele daaropvolgende aanbesteding?	Nee, in het kader van de AVG blijkt dit heel lastig te zijn in de praktijk, helemaal aangezien deze opdracht toegang kan verschaffen tot gevoelige bedrijfsgegevens/privacy.
11	dCI-000492	Mogen wij voorbeelddocumenten als referentie meesturen bij onze antwoorden op de marktconsultatievragenlijst?	Uiteraard.
12	dCI-000492	Indien voorbeelddocumenten zijn toegestaan, mogen deze dan in het Engels worden ingediend?	Als voorbeeld prima, maar bij de mogelijke aanbesteding dient dit in het Nederlands te zijn.
13	dCI-000492	Vragen vanaf deze vraag hebben betrekking op de afbakening, zodat wij u prijsindicaties op hoofdlijnen kunnen geven. Kunt u een ruwe schatting geven van het aantal externe doelwitten (bijv. servers, routers, firewalls) binnen de scope? Een totaalaantal (IP-aantal) is voldoende.	Het IP aantal extern is ongeveer 50. Het IP aantal intern is ongeveer 1500 (loopt uiteen van servers, databases, switches, werkstations, accespoints, printers, etc.). Het IP aantal IoT is onbekend tot op heden.
14	dCI-000492	Kunt u een ruwe schatting geven van het aantal interne doelwitten (bijv. servers, routers, firewalls, switches) binnen de scope? Een totaalaantal (IP-aantal) is voldoende.	Het IP aantal extern is ongeveer 50 Het IP aantal intern is ongeveer 1500 (loopt uiteen van servers, databases, switches, werkstations, accespoints, printers, etc.) Het IP aantal IoT is onbekend tot op heden
15	dCI-000492	Bevat de scope van de penetratietest ook een hardwarebeveiligingsbeoordeling van embedded apparaten binnen het IoT-netwerk?	In principe niet, tenzij de pentester iets heel opvallends tegen het lijf loopt voor wat betreft hardware/embedded apparaten.
16	dCI-000492	Als het antwoord op vraag 8 “Ja” is, is het dan mogelijk om de IoT-apparaten naar onze locatie te sturen voor testen, of is ter plaatse testen vereist?	Nee dit is niet mogelijk. De opdracht dient hier ter plaatse te worden uitgevoerd.
17	dCI-000492	Als het antwoord op vraag 8 “Ja” is, omvat de scope dan het demonteren van het IoT-apparaat en het uitvoeren van een directe beoordeling op het moederbord?	Nee, wat u aangeeft is niet inbegrepen in de scope van deze opdracht.
18	dCI-000492	Bevat de scope de beoordeling van de radioprotocollen (zoals BLE, WiFi) die op het IoT-apparaat draaien?	In principe niet, tenzij de pentester iets heel opvallends tegen het lijf loopt voor wat betreft BLE/Wifi.
19	dCI-000492	Wordt de firmware-binaire of de broncode beschikbaar gesteld voor softwarematige kwetsbaarheidsanalyse?	Nee.
20	dCI-000492	Is remote testen acceptabel, of wenst u testen ter plaatse?	Extern kan remote (blackbox), maar intern en IoT ter plaatse.
21		Worden specifieke kwaliteitsstandaarden zoals het CCV-keurmerk voor pentesten betrokken in de afweging bij een toekomstige aanbesteding?	Ja, het CCV-keurmerk wordt opgenomen als minimumeis.

22		Wat is de breedte waaronder we de term pentesten moeten verstaan. Vallen hier bijvoorbeeld ook Red/Purple/Blackteaming opdrachten onder? Of beperkt het zich tot alleen technische en functionele onderdelen in het IT-landschap.	De pentest beperkt zich tot alleen technische en functionele onderdelen in het IT-landschap.
23		Omdat wij een nadrukkelijke samenhang zien tussen het uitvoeren van de pentest en het verwerken van de uitkomsten besteden wij altijd veel aandacht aan mitigerende maatregelen en adviezen hieromtrent. Vormen daarom adviestrajecten zoals bijvoorbeeld een Cybercrisis Readiness Assessment ook een onderdeel van de gevraagde diensten?	De gemeente is op zoek naar aanbevelingen voortvloeiend uit de pentest. Mogelijk wordt de vormgeving hiervoor een gunningcriterium.
24		Overweegt de gemeente een meer gefaseerde aanpak waarin ieder jaar een ander domein (extern, intern, IoT) centraal staat, om spreiding en verdieping mogelijk te maken?	Het eerste jaar willen we een algemene pentest voor extern, intern en IoT om een totaalbeeld te krijgen. In het jaar daarop kunnen we hierover in overleg treden waar de focus op komt te liggen.
25		Wordt een verwerkersovereenkomst vereist voor partijen die tijdens de pentest toegang kunnen krijgen tot persoonsgegevens?	Ja, de gemeente is verplicht de IBD standaard verwerkersovereenkomst voor gemeenten toe te passen.