Questions & Answers 1 – PQD IT/09/DT/AG/20 – Provision of Deception Technology Services

16.09.2020

Question 1	**3.5 Reliance on Third Parties** - specifically with the section on subcontracting. **Can a Deception Technology Vendor participate in multiple proposals as a subcontractor to a Service Provider?** An example is as follows: Deception Technology Vendor (A) participates as a sub-contractor to Managed Service Provider (B) in B's proposal. A also participates as a sub-contractor to Managed Service Provider (C) in C's proposal. Vendor A appears in two Service Provider proposals (B and C's) as a subcontracted Deception Technology Vendor. It is clear in the section on consortium that this is not the spirit of acceptable behaviour for consortiums, could the ESM please clarify if this behaviour is acceptable in the case of subcontracting agreements.
Answer 1	**Yes, there is no restriction for one subcontractor to participate in this procurement procedure and submit a proposal together with one or more candidates. Please note that in case the candidate intends to subcontract some of the services, specific evidence should be provided as indicated in the Section 3.5 of the PQD.** **Candidates are reminded of the content of the Non-Collusion Declaration pursuant to which Candidates must prepare their application autonomously and independently, do not divulge, discuss or compare their application with other Candidates taking part in this procurement process and do not contact or collude with other Candidates with the purpose of distorting competition. Candidates need to take appropriate and necessary measures to ensure that their subcontractors or other third parties involved respect the same rules and principles.**
Question 2	**Preference for Vendor or Service Provider led proposals** We see two main possibilities for collaborations using subcontracting arrangements to fulfil the requirements: (A) A Managed Service Provider makes a main proposal and uses a Deception Technology Vendor to fulfil certain aspects of the requirements as a sub-contracted entity. Or (B) the reverse, the Deception Technology Vendor makes a main proposal and uses a Managed Service Provider to fulfil certain aspects of the requirements as a sub-contracted entity. Does the ESM have any preference for either option (A) or (B)?
Answer 2	**Option (B) is the preferred option.**
Question 3	**Lead a proposal and subcontract in another** Can a Deception Technology Vendor participate in a proposal as a subcontractor to a Managed Service Provider, and also present another proposal where the Deception Technology Vendor is the Candidate in its own name? We see this is explicitly ruled out for consortium bids, but this has not been clarified for sub-contracted bids.
Answer 3	**See the Answer 1 above**.

Question 4	Would the ESM integrate the deception solution with ESM's SIEM and will the ESM SIEM/SOC team handle security events?
Answer 4	**The candidates may propose a SOC support as an optional Work Package. The ESM may consider to integrate the deception solution with ESM's SIEM and ask the ESM SOC team to handle security events. Further approach will be defined in the RFP (Stage 2). The RFP will be sent to all pre-qualified Candidates. As defined in Section 3.9, Candidates must achieve a rating of "Pass" for all the "Pass / Fail" criteria to be considered successful at Stage 1 (pre-qualified Candidates).**
Question 5	Does the MSP engineer need to be located within the EU?
Answer 5	**The MSP engineer should preferably be based in the EU, that the time zones are not too different for support purposes. Please note that the Candidates are invited to respond to the questions "For information only items" listed on page 25 of the PQD.**
Question 6	Is the managed service related to the deception architecture, or is this for operational events as well?
Answer 6	**The managed service should also cover operational events as much as possible. Operational events required on devices not managed by the Service Provider (such as opening firewall rules) will be performed by the ESM.**
Question 7	Does the ESM have a list of integration technologies / partners that they can share with us?
Answer 7	**The ESM does not have a list of integration technologies / partners that can be shared.**
Question 8	In the Section "3.2 Overview of the Procurement Requirement (page 4)" there are 2 bullets regarding the objectives. We would like to know if the ESM would consider an interesting added value a third one related to "Detecting external attackers which are trying to break the perimeter of the ESM
Answer 8	**The Candidates may propose such additional work package. However, we do not want to expose Deceptive Artefacts to internet in order to avoid increasing our exposure to internet. Further approach will be defined in the RFP (Stage 2). The RFP will be sent to all pre-qualified Candidates. As defined in section 3.9, Candidates must achieve a rating of "Pass" for all the "Pass / Fail" criteria to be considered successful at Stage 1 (pre-qualified Candidates).**
Question 9	In the section "3.9 Eligibility, Exclusion and Selection Criteria (page 7)" is stated that "In the event that the Candidate submits an Application together with a third party/-ies and/or with sub-contractor(s), the combined capacities of the Candidate and all such third party/-ies and/or subcontractor(s)will be assessed for the purpose of meeting the selection criteria". We have considered combining our capacities with one of the providers based on our previous experiences with them and its technology providing Deception Services globally. We would like to confirm if such combined capacities include any of the requirements established in this Pre-Qualification Document or if there are exceptions.
Answer 9	**It is acceptable to submit applications with third parties. All requirements are set out in section 3.5 of the PQD on page 9.**
Question 10	In the "Annex 1 - TERMS OF REFERENCE, under point 1 (page 12)", it is stated that "The ESM is currently migrating on-premise Microsoft servers to the public cloud of Office 365

	(for Exchange and Sharepoint) and subscribing to new services on the public cloud of Office 365 (for Teams)".We would like to confirm if there is a future plan to migrate the Active Directory or this will remain on the ESM infrastructure.
Answer 10	**The Active Directory will remain on the ESM infrastructure.**
Question 11	In the "Annex 1 - TERMS OF REFERENCE, under point 4 (page 13)", it is stated that "The service provider will be required to provide the following services: Provide all licenses, appliances and/or cloud instances (where applicable required for the solution". Regarding the Deceptive Artifacts there are some times that we need to deploy them via Virtual Machines. Is it possible to run these VM on the ESM Virtual Infrastructure / Hypervisor, or does ESM require to deploy an appliance to virtualize the Deceptive Artifacts? We would also like to confirm that the Licenses would be acquired by us and then used to provide the service.
Answer 11	**Virtual Machines can be run on the ESM Virtual Infrastructure / Hypervisor or in a separate appliance. Therefore, both options can be considered.**
Question 12	We currently provide Decept on Services to other customers with another provider as Technology Partner, and we have a Deception Console multi tenant deployed in our Cloud environment, with all the security measures needed and also with customer isolation. The customers do not have access to the Console, only our CounterIntelligence Team has access. And the data is also isolated between customers instances. We would like to confirm that this approach (a multi-tenant console) is approved by the ESM, or if the ESM does require an exclusive console for the project.
Answer 12	**The ESM prefers an exclusive console for the project. A multi-tenant console can still be considered.**
Question 13	Please confirm the number if the number of production servers in the DR Site is same (150) as in the datacenter? (“ANNEX 1 - TERMS OF REFERENCES - Section- Para 4).
Answer 13	**There are no production servers in the DR site. Staff is provided with the place to ensure business continuity in the DR site. Please refer to Answer 19 below for further details on the failover data centre.**
Question 14	Can we share anonymised purchase order screenshots and/or references? Many of our customers have given anonymised feedback on our peer insights page.
Answer 14	**Yes, the customers’ data may be anonymised. The Candidates are advised to include value, size and duration of the references. Anonymised feedback provided in the peer insights page can be taken into account as references if the Candidate presents minimum three (3) and maximum five (5) references from the last three (3) years prior to the publication date of this procurement procedure. Please refer to the Section 2.2– ‘Technical or professional ability’ on page 23 of the PQD for further information**
Question 15	Could the ESM share the organisation who is currently managing and running the SOC?
Answer 15	**We are not able to share this information at this stage.**
Question 16	The SPLUNK SIEM previously alluded to in previous questions, is this solution hosted by the current SOC provider, or hosted internally at ESM? Could the structure and workflow of this arrangement be explained in more detail.
Answer 16	**The Splunk SIEM is hosted by the current SOC provider. Logs of servers, workstations and network equipment are sent with a Splunk universal forwarder. Additional alerts and logs are also collected from cloud-based applications. Further details can be shared at a later stage of the procurement process.**
Question 17	How large is the SOC team? (it is useful to know so we can provide training as part of solution).
Answer 17	**Up to 5 members will participate in the SOC training.**

Question 18	How many people from the ESM IT Security Team, and IT Operations team and Cloud team will be involved in the deception project?
Answer 18	**The ESM IT Security Team consists of 3 people and IT Operations/Cloud Team consists of 8 people.**
Question 19	The data centre architecture – is this passive/active or active active? Is deception required as a part of the failover DC?
Answer 19	**The data centre architecture is active and passive. We do not foresee to deploy deceptive artefacts in the failover DC.**
Question 20	Can you describe the physical locations associated with the proposed implementation? What are the Numbers for remote locations and User locations?
Answer 20	**The Data Centre and the ESM office are located in Luxembourg. The DR site also located in Luxembourg may be considered. Users are located in the ESM office in Luxembourg and users can also be connected remotely with a VPN. There are around 300 users. Thus, there will be between 2 to 3 locations to be covered.**
Question 21	Do we need a „Professionals of the Financial Sector (PSF)“ certification**?**
Answer 21	**We do not require the Candidate to provide a PSF certification.**
Question 22	On Page 23, 2.2 (…e.g. letters/emails of recommendations from previous clients): Our customers don't want to communicate that they are using Deception. How far can they be anonymized as an organization or as a company?
Answer 22	**Please see Answer 14 above.**