Questions and Answers (Q&A)

in relation to the Request for Quotation to support in selecting the Security Incident and Event Management (SIEM) system and approach to be implemented at the OSCE

No.	Question from the Market Operator	Answer from the SIEM Project Team/ Procurement and Contracting Unit
Q&A 1–12 release date: 15 February 2018		
1.	You would appear to have a clear and documented target overall end game in terms of strategy/objectives/processes/technical architecture for your cybersecurity capabilities including a clear understanding as to how SIEM fits, including the reasons/ issues underpinning your decision that a SIEM solution is required. Can you share this with us?	Can be shared after contracting.
2.	How do you see SIEM fitting within your overall cybersecurity program - for example are there interdependencies with other elements of the program?	One of the most critical activities in the program is the procurement and implementation of an ICT security incident and event management tool (SIEM) or managed information security services (MSS) OSCE wide to provide early detection and management of security incidents. There are some interdependencies with other activities; the most important one is the upgrade of our Microsoft infrastructure.
3.	Do you have up to date information on your current infrastructure, cybersecurity processes and can you share this in advance? Rigorous and current asset management is needed here. We are mindful you envision the timeframe for activity 1 to be two months and we see this as only feasible if this information is readily available.	This information cannot be shared in advance. Documentation of the infrastructure is scarce and interviews with system administrators will be required. Security incident processes exist.
4.	Would you please describe your current CyberDefence team in terms of numbers, skills, experience levels, roles performed and degree to which it is centralised versus dispersed.	This information can be only shared after contracting.
5.	Would you please describe the degree to which your organisation is experienced with cloud computing and whether there	We have implemented some cloud solutions in the last two years and have a high-level policy on cloud solutions. These comply with general

	are any restrictions on using latest cloud cyber security offerings? I am wondering whether there is an open field here or imposed restrictions?	practices.
6.	Are you currently tracking incidents/events and would it be possible to share recent information including severity information? If you feel it necessary we will be happy to sign confidentiality agreements in advance of receiving any information on this aspect.	Major security incidents are tracked and documented. Others are documented in our ticketing system but this is not always consistent.
7.	I note with interest you list Kaspersky AV among your security systems. In light of recent events in western world to stop usage of this system due to claimed Russian influence, has a conscious decision been made to continue using the system in spite of these warning?	No answer – I do not see why this information is necessary for bidding.
8.	You mention various locations where there are data centres and internet connections. Can you share a current up to date map of these including the types of systems operating in these locations. This has material relevance on the volumes of data likely to be gathered on a daily basis with SIEM systems.	This will be provided after contracting.
9.	Reference is made to your procurement organisation. Can you share if you have a separate IT Procurement organisation or whether IT procurement is managed within the general procurement organisation?	The Procurement and Contracting Unit (PCU) at the OSCE Secretariat is providing procurement and contracting support in the acquisition of various goods and services, including the IT category of spend. The PCU is positioned in the Department for Management and Finance /Mission Support Services. For more information about the procurement and contracting function at the OSCE please visit https://procurement.osce.org
10.	How many end users are supported by the organisation and what is their geographic distribution?	We have about 4000 end users across Europe and Central Asia. Biggest locations are Secretariat (400 users), Ukraine (1500), Kosovo (500), Warsaw (300) and Bosnia (400). Rest is distributed on the smaller locations (altogether we have 22 locations).
11.	What is the size of your internal IT organisation and again its geographic distribution?	At the Secretariat (which is the provider of central services to all OSCE) we have 32 ICT staff. Altogether we have 150 ICT staff across OSCE, with staff ranging from 40 to 1.
12.	To what extent are third party contractors used within the overall and IT organisations.	We have several consultants and external companies working for OSCE. Majority of the infrastructure operations work is still performed internally.

Q&A 13–12 release date: 21 February 2018		
13.	**Managed Information Security Service** If I understand it correctly, the answer to question 2 raises the possibility that OSCE is considering contracting for a managed Information Security Service (a SIEM service) as an alternative to acquiring a tool for SIEM as contemplated in your RFQ. It is clear from the documentation provided that the "SIEM Consultant" involved in SIEM tool selection would not be allowed to the tender for the actual purchase of SIEM system. We would appreciate clarification on two related points. First, how and when will OSCE determine whether to pursue the SIEM service option? (A) Will this be done in parallel or is the service option considered to be a fallback to the purchase option? Second (B), if the decision was made to go with a SIEM service would the "SIEM Consultant" working on the product selection be considered as a provisioner of the SIEM service and thus disqualified from offering a SIEM service? We believe that (company name removed) is equally qualified to do both the SIEM Consultant role and also provide a SIEM service, and if it is not possible to do both roles then we would have to make an early decision on what element to focus on. Please advise whether it would be permissible to participate on both elements should a decision be made to go with a SIEM service.	(A): According to the ToR, it is part of the Consultant's task to analyse the SIEM as a service option and provide a recommendation to the OSCE. (B): The SIEM consultant will NOT work on the SIEM product selection. The provider and the product will be chosen later as part of an open tender based on the Terms of Reference and requirements developed by the Consultant. The company providing the consultant cannot participate on the tender for the actual solution due to conflict of interest.
14.	**Advanced Persistent Threat (APT)** Your Terms of Reference make particular reference to addressing the risks of Advanced Persistent Threat (APT) attacks. We have considerable experience in responding to APT attacks. These attacks have been widespread for many years now and have grown in stealth and sophistication over the years. Our experience is that it is highly probable that many organisations such as OSCE have been compromised already. This means that simply implementing a SIEM system	Thank you for the notification. These steps were already performed and SIEM is only one (although very important) initiative of a multi-year program to increase the cybersecurity of the OSCE.

	may not offer the protection needed. We would recommend that forensic work be carried out ahead of implementing a SIEM tool or service. My question is whether you contemplate such a precautionary step ahead of implementing SIEM?	
15.	**Asset Inventory** The answer to question 3 says that documentation of infrastructure is scarce and interviews with system administrators will be required. I don't see interviewing administrators as adequate to collect the required information. Our experience is that, nowadays with end users who are capable of installing their own applications without IT involvement, system administrators cannot definitively know what is installed on their infrastructure. This is better addressed using automated tools to uncover and verify what is on the infrastructure. This provides the critical level of confidence and assurance that all vulnerabilities have been identified. An accurate asset management inventory also is needed to estimate the amount of data that a SIEM system will generate, and to size the required system properly. My question is whether you have or will consider such a forensic effort as an important step early in the process. I see this as rather essential if you are to achieve a robustly secure environment.	Please present in detail the approach deemed the best by you in your offer along with resource and other requirements on OSCE side.
16.	As outlined in the ToR, you are expecting the service provider to define use cases for the SIEM solution and to develop a 2-3 years implementation roadmap (p. 3). The high-level phases should encompass 5-10 use cases (p. 4). Based on the information, we have following questions: (A) How many different use cases do you expect in total? (B) How many phases do you expect?	(A): We do not have any estimate on the number of use cases yet. (B) We were calculating so far with 6-month long phases (5-10 use cases each) for 2-3 years.

END.