

B		SOC Queries, Response and Clarifications	
Sr.No	Query	PTA Response	
1	Earnest Money 4% in shape of Bank guarantee may also be allowed along with DD/PO or DAC , Can a firm apply for SOC and DS Switch ?	Bank Gurantees are not allowed. Both Company and Firm can apply for SOC and DS Switch only. Registration certificates and NTN/STN apply.	
2	How many DLP end points required.	100 users, 75 Servers, Based on Windows and Linux machines, covering email services, File servers, oracle databases, postgres data base, MS Sql Server, Web Servers etc, futhermore all client devices will be integrated at Phase-II.	
3	How many EDR end points required.	100 users75 Servers only (32 Physical and 43 Virtual Machines/Containarized Servers), Furthermore, in phase-II all devices including clients will be covered.	
4	Can we provide on cloud deplyment solution that will save cost of Infrastructure.	The solution should be on premisses only.	
5	Can we provide complete solution based on SAAS (Software as a Service Model for (03) years)	SAAS Models are not allowed , solution must be on premisses.	
6	Who will provide hardware for all components of the SOC	PTA Will provide the Hardware. However, vendor to provide the required specifications of the Hardware	
7	Currently it is asked for 10K EPS but from the list of their Hardware , database and application, it seems 10K EPS is on higher end? Have they done any sizing activity for this EPS and can they share this sizing sheet? If the requirement is the same list of infra, database and application? can we do our own sizing to ensure we cover all these?	A minimum of 5000 EPS shall be covered / quoted by all vendors,however, the system must have capbility to support 10000 EPS or above in future phae-II upgrae.	
8	Is there any PAM solution running ? If yes, its name ?	No PAM Solution is running at this point in time.	
9	The SOC is used for PTA infra already shared or it will be used for any external usage as well ?	The SOC will be used for Internal usage only.	
10	In the scope of the work , it is mentioned 01-year OEM support but asked for 03 years support? How can be OEM support be 01 years and 03 years ? Please clarify how many years of support is required.	Typo mistake, support is requied from partners of the priciple manufacturers for 3 years 24 X 7. Further to clarify that Manage support services from priciple manufacturer are not required , whereas, vendors will be responsible for support from OEM.	
11	You have mentioned RE for 01 year only ? Whereas support is for 03 years? Please clarifiy.	The main purpose of resident engineer is to colloborate/laison and get support from principle manufacturer and in the mean time to get train PTA resources to execute daya to day activities, further, support and Software updates remains 3 years 24 X 7. Software licences shall be perpetual.	
12	Number of users	The question is not clear , however, 75 servers needs to be coverd, including VMs, containarized machines running on Ubuntu linux, email services running on Redhat linux, Windows File servers, postgre sql running on ubuntu linux, Oracle DB on both windows and Linux , MS SQL DB servers .etc.	
13	Number of branches	12 X Zonal offices,Headquarter and camp Office, Total = 14.	
14	Are the mentioned log sources located in HQ only, or HQ and DR site	Both locations.	
15	Firewall models	Forigate 240D =1, Fortigate 600D =1, Fortigate 100d = 7, Fortigate 100E =2, PAN 3220 =2, Barracuda Spam Firewall =1, FortiWAF 1000E =1. Juniper SRX Firewall =2.	
16	Are Firewalls deployed as Active/ Active or Active/Passive ?	Active/Active.	
17	Current/EPS of known.	Please conduct a survey. However a minimum of 5000 EPS should be covered.	
18	Are there any specific requirments for online requirments for online logs retention period?	Live logs will be kept for 30 days.	
19	Is there any complaince required ?	Complaince will be carried out in future Phase-II,not at this point in time.	
20	Should the offering be software or hardware or both options?	Software option only.	
21	Is there a disaster recovery or High availability requirement for SIEM?	Software backups will be taken from time to time currently HA is not required. However, in phase-II HA functionality will be required.	
22	Is there any house built applications or any other log sources that not mentioned in the tender?	Currently up to 20 house build custom applications will be covered by the solution and Database activity monitoring capability is required both for privileged users and normal DB activities.	
23	How many and which type of Databases will be there in the envornment with respect to user behaviour analytics ?	Number of Postgre SQL Databases are = (5) , Number of Oracle Databases are = (4), Number of Microsoft SQL Server Databases are = (4).	
24	Kindly clarify the user value unit (Authorized User) License + SW subscription & support 12 months for SOAR?	(2) Authorized users licences are required, Software license should be perpetual with (3) years support and updates from partners. Managed support from principle manufacturers are not required.	
25	What type of trainings are required?	SIEM Training, Furthermore, SIEM Solution Should exist in Gartner Magic Quadarant Leaders, report 2020.	
26	Certificate of prohibited origin.	Certificate must to be provided stating that no part of Hardware and Software has been manufacturer/assembled or developed in India and Israel.	