

Corrigendum and Addendum to Request For Proposal (RFP) for supply / Installation of Central Log Management Solutions

Corrigendum:

SI No.	Clause No.	Existing RFP Clause	New RFP Clause
1.	Page 19 – Clause 5.1	The solution must be in a position to fetch the data from the real time updated global repository on the information of latest threats and resolution details to keep in pace with the latest threat outburst. The system should have the correlation capability with the global intelligence feeds.	The clause will be read as under: The solution must be updated regularly on the information of latest threats and resolution details to keep in pace with the latest threat outburst. The system should have the correlation capability with the latest / new threats/ information.
2.	5.1.IV.2.d (Page No 20)	Log Reduction should remove unneeded entries from a log to create a new log that is smaller.	Removed from the RFP
3.	5.1.IV.2.e (Page No 20)	Log Conversion should facilitate parsing a log in one format and storing its entries in a second format.	Removed from the RFP
4.	5.2 (Page No 21)	The solution should ship as solution in a box so as to give flexibility in deployment options. It should have non-windows hardened platform to minimize the security breaches and database should be included with in the solution which should not be non-proprietary.	The clause will be read as under: The solution should ship as solution in a box so as to give flexibility in deployment options. It should be hardened to minimize the security breaches and database should be included within the solution which should not be non-proprietary. The required client access licences, if any, must be included with the solution.
5.	7.d (Page No 25)	Specific experience of the Bidder relevant to implementation & maintenance of Central Logging Management system for Banks, FIs , Govt., PSUs, LC*	Central Logging Management system will be read as Security Solutions .

6.	Annexure-1 , Part 2 (Alerting and Correlation (Page No 37)	The system should have a web based reporting console for monitoring and managing the SIEM solution and devices that are sending logs to the solution.	The para will be read as under : The system should have a web based reporting console for monitoring. Provision for managing the SIEM solution and devices that are sending logs to the solution must be available.
7.	Annexure-1 , Part 2 (Alerting and Correlation (Page No 37)	The raw logs should be time stamped, compressed and encrypted before being written to the storage.	The clause will be read as under: The raw logs should be time stamped, compressed and encrypted.
8.	Annexure-1 , Part 2 (Alerting and Correlation (Page No 37)	The system should allow sending alerts to administrators using emails alerts, syslog notifications SNMP traps. Also the ability to forward alerts via Syslog,SNPP and SNMP.	The clause will be read as under: The system should allow sending alerts to administrators using emails alerts/ syslog notifications /SNMP traps. Also the ability to forward alerts via Syslog/SNPP/SNMP.
9.	Annexure-1 , Part 2 (Alerting and Correlation (Page No 38)	The system/solution have the ability to correlate all the fields in a log without normalizing the logs at collection points.	The clause will be read as under: The system/solution has the ability to correlate all the fields in a log with/without normalizing the logs at collection points.
10.	Annexure -1 , Part 2 (Alerting and Correlation) [Page No 38]	The system should allow a wizard based interface for rule creation. The rules should support logical operators for specifying various conditions in rules.	The clause will be read as under: The system should permit new rule creation. The rules should support logical operators for specifying various conditions in rules.

Addendum :

SI No	In addition to the existing clauses following clauses are being added under product specifications.
1.	The solution must have provision for minimum of 1 TB storage space.
2.	There should be secured communication between the central management server and the clients.