CORRIGENDUM - 6

1. REVISED TERMS & CONDITIONS (Forming Part of Original RFP)

REVISED TERMS & CONDITIONS (Forming part of Original RFP)

TECH SPEC

Existing Clause: (Pg. No. 19 - Corrigendum 4; Pg. No. 90 – Original RFP)

The log collection engine should have high availability without depending on third party solution. Logging and correlation modules should be proposed in standalone.

UIIC's reply to pre-bid queries: - All components needed for the Solution should be in HA.

UIIC clarification:

The Bidder is required to propose the SIEM with standalone instance at DC & DR, except log collector which should be in HA at DC and HA at DR.

Existing Clause: (Pg. No. 21, Corrigendum 4; Pg. No. 95 – Original RFP)

The solution should have high availability feature built in. There should be an automated switch over to secondary SIEM in case of failure on the primary SIEM. No performance degradation is permissible in case of failure.

UIIC's reply to pre-bid queries: - SIEM solution with all components in HA in DC and HA in DR

UIIC clarification:

The Bidder is required to propose the SIEM with standalone instance at DC & DR, except log collector which should be in HA at DC and HA at DR.

Existing Clause: (Pg. No. 20, Corrigendum 4; Pg. No. 95 – Original RFP)

System should have inspection throughput of 500Mbps and scalable to 2 Gbps without additional hardware

UIIC's reply to pre-bid queries: - System should have inspection throughput of 500Mbps and scalable to 2 Gbps without additional hardware.

System should have high performance architecture that ensures that attack mitigation does not affect normal traffic processing and should support DDoS Flood Attack Prevention Rate up to 15 Million PPS.

UIIC clarification:

System should have inspection throughput of 500Mbps and scalable to 2 Gbps without additional hardware.

"System should have high performance architecture that ensures that attack mitigation does not affect normal traffic processing and should support DDoS Flood Attack Prevention Rate up to 15 Million PPS" – **This clause in italic font stands deleted**

Existing Clause: (Pg. No. 43, Corrigendum 4)

Bidder to provide the packet capture solution in standalone mode at DC & DR. Throughput of 1 Gbps with retention period of 7 days for raw logs and 30 day meta. Bidder should integrate the packet solution with SIEM and provide integrated view of logs and packets.

Revised Clause:

Clause stands deleted

3.2.4.7 F. Next Generation Firewall

Existing Clause: (Pg. No. 48, Corrigendum 4)

Support for application information feed: The solution must provide an application control function that must allow for the importation and use of information about applications. The feed should include information about how applications are used and provide recommendations to the customer regarding actions to take if the application is discovered in use. There shall be minimum 7000+ application control.

Revised Clause:

Support for application information feed: The solution must provide an application control function that must allow for the importation and use of information about applications. The feed should include information about how applications are used and provide recommendations to the customer regarding actions to take if the application is discovered in use. There shall be minimum 4000+ application control.

3.2.4.7 F. Next Generation Firewall

Existing Clause: (Pg. No. 48, Corrigendum 4)

There shall be Data Classification control for minimum 600+ Data Types.

Revised Clause:

Clause stands deleted

3.2.4.7 F. Next Generation Firewall

Existing Clause: (Pg. No. 50, Corrigendum 4)

The solution must include Four (4) 10Gbps (SFP) and Four (4) 1 GBPs (SFP) and 8x 10/100/1000Base-T RJ45 port card copper interface requirements from the Day1.

Revised Clause:

The solution must include Two (2) 10Gbps (SFP/SFP+) and Four (4) 1 Gbps (SFP) and 8x 10/100/1000Base-T RJ45 port card copper interface requirements from the Day1.

3.2.4.7 F. Next Generation Firewall

Existing Clause: (Pg. No. 50, Corrigendum 4)

The solution must have min 32 Gb RAM in both primary & HA firewalls Should have minimum 240 GB of SSD on both primary & HA firewalls.

Revised Clause:

The solution must have min 16 Gb RAM in both primary & HA firewalls Should have minimum 240 GB of SSD on both primary & HA firewalls.

2. UIIC's clarifications

Please find below, UIIC's clarifications for some of the replies with reference to Corrigendum 4 (for replies to pre-bid queries).

Point/section	UIIC reply in Corrigendum 4	UIIC's explanation
Pg. 24 of corrigendum 4 3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)	SIEM should handle data burst/beyond peak EPS and should not drop logs. Peak EPS should be double the sustained EPS	UIIC wants SIEM not to drop logs and should handle peaks EPS as mentioned. If this feature meets the requirements, bidder can propose. If peak EPS is not handled as per its requirement at any stage of the contract period, bidder has to provide the same without any commercial to UIIC.
Pg. 19 of corrigendum 4 ANNEXURE 10 - TECHNICAL AND FUNCTIONAL SPECIFICATIONS - SIEM, Point no. 1	The Solution should be an appliance based with a clear physical or logical separation of the collection module, logging module and correlation module. OEM should confirm all the appliances are sized for sustained 20,000 EPS. Appliance means purpose built hardware with all requisite OS and security application pre deployed at OEM manufacturing facility and shipped from there manufacturing location.	UIIC wants purpose built appliance. Collectors can be virtual appliance.
Pg. 43 of corrigendum 4	xxi. Bidder to provide ITSM tool with device monitoring for minimum 100 devices (network/security devices) including devices proposed in this RFP at no additional cost to UIIC.	Bidder needs to provide ITSM with device monitoring tool for 100 devices monitoring along with 5 ITSM Users license. The EMS needed for the proposed devices (100 devices) will be coming under the scope of bidder.
Pg. 21 of corrigendum 4	The solution should support creation of incident management workflows to track incident from creation to closure, provide reports on pending incidents, permit upload of related evidences such as screenshots etc. Solution should have inbuilt capability and should support Integration with external ticketing tool. UIIC does not have any ITSM tool.	Bidder needs to provide ITSM with device monitoring tool for 100 devices monitoring along with 5 ITSM Users license.

<u>Note:</u> *Apart from these clarifications & explanation, clarifications provided in Corrigendum 4 are considered as a part of original RFP.*

2. Extension of Bid Submission Date

REQUEST FOR PROPOSAL (RFP) FOR SUPPLY, INSTALLATION, IMPLEMENTATION, INTEGRATION, MAINTENANCE AND SUPPORT OF SECURITY SYSTEM (RFP No. 000100/HO IT/RFP/138/2020-21)

Extension of bid submission date

This is further to our tender reference no. 000100/HO IT/RFP/138/2020-21 dated 13.08.2020 issued for procurement of ‘Captive Security Operations Center and Dedicated SIEM tool’.

The last date of bid submission is extended to 26.11.2020 (03:00 PM).