Corrigendum - 01 : Response to pre-bid queries

Date:27th June 2024

RFP Ref :No: NESL/AO/ISD/RFP-eASM/2024-25/240601 dated 20th June 2024

Sl.NO	RFP Page Number	Section/ Clause	Present clause in RFP	Query Description	NeSL Response	Amendments, if any
1	5	10	**Infrastructure Monitoring:** Continuous scanning and monitoring of IP assets and web applications. Discovery of all public facing assets which are exposed to Internet. Solution shall monitor NeSL domain, its subdomains, web apps, and IP addresses associated with the given domain.	Please provide the top main and alternate domains that are required to be monitored?	One main domain details shall be provided with succesful bidder. The monitoring shall be available for all its sub-domains, Web apps and IP addresses associated with this domain.	Nil
2	5	10	**Email Health:** Monitoring email domains and accounts for signs of compromise, phishing attacks, spam activity, and email authentication issues including checking DNS and SMTP configuration issues.	ASM and Dark web monitoring solutions help identify compromised emails and phishing domains. However, spam activity, and email authentication issues are outside the scope and more focused towards email security solutions. Could you please amend this line to remove these 2 points?	Clause stands amended as:	**Email Health:** Monitoring email accounts for signs of compromise and phishing attacks.
3	5	10	Advanced vulnerability detection capabilities, including support for CVE databases, common misconfigurations, and emerging threats.	Please elaborate on this line," Support for CVE databases"	Solution should leverage disclosed security vulnerabilities and exposures through CVEs relevant to the monitored assets.	Nil
4	5	10	Integration with threat intelligence feeds to enrich monitoring data and identify emerging threats relevant to the organization.	Is NESL looking for separate Threat feeds	Integration with threat intelligence feeds to provide services envisaged in the RFP shall be made available.	Nil
5	5	10	Comprehensive reporting functionality, including executive summaries, detailed vulnerability reports, trend analysis, and actionable recommendations.	Does NESL want the solution to do Penetration Testing as well	Refer 10 B) - The Solution should check for vulnerabilities, risks, threats and possible attack vectors on the public facing IT assets and its related entities which may lead to attack surface and provide recommendation for mitigation of the threat.	Nil.

6	6	10. A) 4	The ability to integrate with security devices through STIX/TAXII is a desirable feature	Is NESL only looking for integration via STIX TAXII	The integration with security devices though STIX/TAXII is not a mandatory feature, but is desirable. If Bidder solution is having other mechanism for integration with security solutions, it may be highlighted in the proposal.	Nil
7	7	10. A) 5d	**d) Incident Prevention and Response:** Enabling proactive defenses by providing actionable advice on potential security threats and helping to detect, respond to and mitigate incidents more effectively.	Helping to respond to and mitigate incidents more effectively; does NESL want Incident Response service from OEM	Successful Bidder shall provide actionable advice on potential security threats and helping to detect, respond to and mitigate incidents more effectively. Incident response service is not envisaged in this association, other than actionable advices. However, takedown service as defined in RFP is to be provided by the bidder.	Nil