Corrigendum - 8			
NIT NO. CMC/BY/24-25/RS/SkS/APT/48 [RFx Number: 2200000076] for "SUPPLY & IMPLEMENTATION OF SOC SOLUTION INCLUDING TECHNOLOGIES SIEM, SOAR, UEBA, NDR/NBAD, THREAT HUNTING, THREAT INTELLIGENCE, INCIDENT MANAGEMENT FOR BRPL."			
Calrifications			
NIT Page no	**Sr . No**	**NIT Clause Descriptions**	**BYPL Clarification**
106	1.21	The next gen SIEM solution should support high availability features and should be proposed in HA mode for all layers at DC	Complete solution to be in HA incl SIEM, SOAR, NDR (except packet capture layer in NDR). Means NDR central management/correlation layer to be in HA.
105	1.12	The proposed solution must support 1000+ data sources with predefined parsing/normalizations rules out of the box.	The proposed solution must support min 400 data sources with predefined parsing/normalizations rules out of the box.
106	1.20	Next gen SIEM solution should be EPS based and must support logs from unlimited devices or sources	Bidder can also proposed GB or device based solution. Need to justify offered GB/Device versus EPS required in the NIT.
106	1.27	Solution should be appliance/hardened device based and appliance should able to support 20000 EPS without any upgrades from day 1.	Bidder can also proposed VM based solution. But hardware for VM should be factored along with the complete solution and also its performance and in case BYPL experience any performance issue bidder needs to upgrade it free of cost to ensure the performamnce of the complete solution stack.
106	1.28	Hardware and software to be sized by the OEM as bundle with maximum performance guarantee in HA mode. Hardware appliance should be tuned and engineered for the SIEM & SOAR system. OEM should own overall performance responsibility of the system.	Bidder can also proposed VM based solution. But hardware for VM should be factored along with the complete solution and also its performance and in case BYPL experience any performance issue bidder needs to upgrade it free of cost to ensure the performamnce of the complete solution stack.
SIEM			
75	24	Log Management Performance: The proposed solution should have event handling capacity with low capacity incremental blocks.	Ability of a system to process events or tasks in small, manageable units while adhering to constraints on resource usage or throughput. These system are designed to handle workloads incrementally by dividing process into discrete blocks.
76	37	The solution should provide time based and forward feature at each log collection point.	The solution should provide device / time / event / IP based / and forward feature at each log collection point.
78	e	The solution must have at least 25+ out of the box machine learning algorithms for Threat hunting which will execute queries on 24x7 basis	The solution must have at least 15+ out of the box machine learning algorithms with multiple customization parameters for Threat hunting which will execute queries on 24x7 basis
UEBA			
96	2	Said UEBA tool should be able to integrate with Next Generation tools like NDR, SOAR & SIEM solution in future.	UEBA tool is an integral (embedded) part of SIEM Solution itself and also should be able to integrate with NDR (Optional)
96	4	The solution should have permission for device admin, subnet admin, audit log, edit model and advanced search, etc.	The solution should have permission for device admin, subnet admin, audit log, edit model and advanced search, etc. or any other RBAC profiling method.
96	16	Flexibility to configure rolling window of period for behavior profiling	Dynamic rolling window period for behaviour profiling
SOAR			
88	1	The solution must be a fully on-premise solution deployed in house. The OEM to provide the hardware for the proposed solution	The solution must be a fully on-premises solution deployed in house. The bidder to provide the hardware/VM for the proposed solution
90	29	For secure operations, the solution must run various scripts, commands, application functions, playbooks etc without the need of running with elevated privileges on a host OS.	For secure operations, the solution must run various scripts, commands, playbooks etc with only necessary previlages.

90	30	Solution should use playbooks/runbooks with a visual editor/canvas which supports visual creation of playbooks without the need to code by native integration to third party tools and processes.	Solution should use playbooks/runbooks with a visual editor for creation of playbooks without the need to code
91	34	Solution should allow creating new playbooks to map out the CIRT processes. Provision for building min 20 custom playbooks should be factored within the solution	Solution should allow creating new playbooks to map out the necessary regulation processes. Provision for building min 20 (but not limiting to) custom playbooks should be factored within the solution.
91	35	Solution should support re-use of playbooks in bigger playbooks	Solution should support re-use of playbooks in wider scenarios
91	36	Solution Should allow creation of Manual Tasks, Automated Tasks and Conditional Tasks in Playbooks	Solution Should allow creation of Manual Tasks, Automated Tasks in Playbooks
91	38	Solution should allow a complete playbook to be run automatically or manually and list out any exceptions	Solution should allow a complete playbook to be run automatically or manually
91	39	Solution must support step by step debugging of the running playbooks with provision of starting from where it stopped on error	Solution must support step by step detailing of the running playbooks
91	40	Solution should record all manual and automated entries during execution of a playbook	Solution should record all entries during execution of a playbook
91	42	Solution must support provision to pass parameters to upstream/downstream task within a playbook.	Solution must support provision to pass proceedure to upstream/downstream task within a playbook.
92	56	Solution should maintain SLA for incident	The solution must measure SLA for the incident.
93	73	The system should be able to extract IOCs from PDF/csv/other formats and search for those IOCs within the organization raw data. In case IOC is found, the system should trigger a new alert and save the indicator information in the local IOC Database.	The system should be able to extract IOCs from csv/ txt/ stix and taxii format.
93	74	The system should support creation of an incident based on an email input (e.g. analyse all emails from a dedicated phishing mailbox)	The system should support creation of an incident based on an email extract input
95	98	SOAR should have an integrated Threat Intelligence Platform (TIP) and should Facilitate importing and parsing structured and unstructured intelligence documents- Structured/finished intelligence analysis reports (.txt, .PDF); Automatically ingest email lists with threat information; Formatted CSV Files, XML-based structured intelligence - STIX	SOAR should be capable to integrate with 3rd party Threat Intelligence Platform (TIP) to enrich the data in csv/ txt/ stix and taxii format.
95	99	TIP should De-duplicate indicator input data when imported from multiple sources; Provide features to add context to and enrich threat intelligence-Ability to rank or assign severity of risk to intelligence and IOCs	SOAR should enrich the data which input from multiple sources and provide features to add context and enrich the threat intelligence
NDR			
102	5.4	The solution should have capability to instruct network security devices such as firewalls to block certain types of traffic, quarantine the host, etc.	This is deleted from NDR and is already part of SOAR
103	7.4	The solution should support the capability to alert the admin and provide mitigation action like quarantine or block the endpoint or custom scripts like ACL push or block the further spread of the malware/worm.	This is deleted from NDR and is already part of SOAR