6. Project Summary

The Institute of Business Administration (IBA) seeks the services of Security Operations Center (SOC) being managed, operated and maintained by third party service provider to enable IBA to prevent, detect, respond and recover from cyber security threats and events.

SIEM & SOC solution up to 100 Assets, including of Vulnerability Scanning, Log Ingestion, Threat feed, 24x7 SOC, Asset discovery

7. Project Objectives

i) Develop related processes and procedures for IBA in order to effectively manage the operations of Security Operations Center (SOC). The processes and procedures should be detailed and easy to understand and follow.
ii) Study IBA's environment to identify attack surface areas.
iii) Review and analyze already established use cases for identification of any anomaly or incompleteness in-respect of threats and identified attack surface areas. Fine tuning and establishment of new use cases should be carried out where necessary.
iv) Monitor and analyze the security event data to reveal / identify any anomaly or incident that can lead to jeopardizing availability, integrity and confidentiality of data.
v) Service provider should have robust threat intelligence mechanism that should be leveraged during detecting and remediating an incident.
vi) Periodic reporting including daily report of events / incidents / attack(s) to the management and desired audiences as per agreed criteria.
vii) In-depth analysis and investigation of an event(s) / incident(s) for forensic analysis.
viii) Perform periodic table top blue team exercises to test the response and resilience level.
ix) SOC services are required for 24 hours per day, 7 days a week and 365 days a year (24x7x365).

8. Technical Specifications

S.No.	Platform Capabilities	Technical Details	Particular Detail Reference Page in Bid	Bidder's Assessment (Y/N)	Alternate Solution (If any)
1	Next Generation SIEM	NG-SIEM Services for servers and Workstation (Solution should equipped with latest feature set like AI, Machine Learning (ML), Network Traffic Analytics (NTA) and User Behavior Analytics (UBA)	TECH. PROPOSAL Pg. 4,6,9 12,13	Y	Doesn't Apply
		Flat per Asset Licensing (Not EPS, MPS/TPS, Log Volume based)	Pg. 6,17	Y	Doesn't Apply
		Cloud SIEM (O365/G-Suite/ AWS & Azure Active Directory)	Pg. 8,10	Y	Doesn't Apply
		Big data backend, Data Lake	Pg. 15,16	Y	Doesn't Apply

		Should have inbuilt Entity Behavior Analytics (EBA) capability	Pg. 8, 9, 12	Y	Doesn't Apply
		Should possess Network Detection and Response (NDR) with up to 1Gbps Traffic Ingestion	Pg. 9, 13	Y	Doesn't Apply
		Should be an XDR based platform	Pg. 6, 9, 12	Y	Doesn't Apply
		Cyber Kill Chain mapping with detection playbooks (New detections should added continuously by the solution provider)	Pg. 12, 13, 14, 15	Y	Doesn't Apply
		Integrated Threat Intelligence	Pg. 12, 13	Y	Doesn't Apply
		Correlation Engine	Pg. 9, 13	Y	Doesn't Apply
		AI/Machine Learning for anomaly detections	Pg. 6, 9, 16	Y	Doesn't Apply
		Log enrichment, Drill Down, Threat Context of Alerts	Pg. 10, 12, 13	Y	Doesn't Apply
		Threat Hunting Module	Pg. 7, 9, 13	Y	Doesn't Apply
		Agents Sensor for Windows, Linux, VMware, Containers, Hyper-V	Pg. 8, 10, 12	Y	Doesn't Apply
		Syslog forwarding	Pg. 8, 10, 19	Y	Doesn't Apply
		Asset discovery (Approved vs Unapproved Assets detections)	Pg. 8, 11, 14	Y	Doesn't Apply
		Services Discovery and Analytics	Pg. 12, 21	Y	Doesn't Apply
		Applications and Protocol Discovery and Analytics	Pg. 21	Y	Doesn't Apply
		Network deep packet inspection	Pg. 8, 12	Y	Doesn't Apply
		One Year full log retention	Pg. 16, 22	Y	Doesn't Apply
		Support Off-Site log Archiving and should be part of solution with no additional cost	Pg. 16	Y	Doesn't Apply
2	Vulnerability Management	The Solution Should be a specialized solution of VA, and have presence in Gartner Magic Quadrant, rather than any simple built-in module.	Pg. 6, 7, 8, 10, 11	Y	Doesn't Apply
		Vulnerability Risk Scoring	Pg. 10, 12, 21	Y	Doesn't Apply
		Active, Passive scanning with real-time visibility of environment changes	Pg. 7, 10, 10, 21	Y	Doesn't Apply
		Policy Assessment (e.g NIST, CIS)	3, 6, 8, 17, 19	Y	Doesn't Apply
		Remediation Reports	10, 21 – 23	Y	Doesn't Apply
		NIST Vulnerability Database	10, 17	Y	Doesn't Apply
		Asset Compliance Dashboard (SCAP)	10, 17, 21	Y	Doesn't Apply
3	Environment Hardening during Installation Phase	The solution must have Minimum 30 Days	17, 19	Y	Doesn't Apply
		handholding/Consultancy as part of proposed solution	17, 19	Y	Doesn't Apply
		IBA Environment Hardening (Help reducing attack surface), based on the guidelines of NIST Cybersecurity Framework (NIST-800)	17, 19	Y	Doesn't Apply
		Assurance of CIS Top 20 Controls Mapping (Reduces Risks) before handing over	17, 19, 21	Y	Doesn't Apply
		Project Supervision by at least CISSP Certified consultant	17, 19, 20	Y	Doesn't Apply
		Use case Development relevant to IBA	Pg. 7	Y	Doesn't Apply

		SIEM Integration, Data point identification	Pg. 6	Y	Doesn't Apply
		Best Practice Recommendations and Anomalies correction guidelines	Pg. 19	Y	Doesn't Apply
		Vulnerability Management System Deployment	7,8,10,17,21	Y	Doesn't Apply
4	SOC Monitoring Services	Solution should have Tiered SOC Monitoring (Global SOC + Regional SOC)	Pg. 14	Y	Doesn't Apply
		24x7x365 SOC threat, event and incident alerting	Pg. 14	Y	Doesn't Apply
		24x7x365 SOC analysis, recommendations, and escalations	Pg. 14	Y	Doesn't Apply
		Vulnerability Remediation Assistance	Pg. 15	Y	Doesn't Apply
		Pervasive Security Visibility via Real-time Dashboards	Pg. 15	Y	Doesn't Apply
		Scheduled vulnerability scanning	10,11,18,22	Y	Doesn't Apply
		Weekly vulnerability reporting vetted by Security Experts	Pg. 10, 22, 18	Y	Doesn't Apply
		On-demand Custom Reports	Pg 22	Y	Doesn't Apply
		CIS20 SOC reports, should be provided on monthly basis	Pg 22	Y	Doesn't Apply
5	SOC Procedures & Policies	The solution should be based on NIST Cybersecurity Framework (NIST-800)	4,7,9,20	Y	Doesn't Apply

Total (Per Year)	PKR. 5,115,000/-
SST	PKR. 869,550/-
Grand Total Amount (Per Year)	PKR. 5,984,550/-

Haris Qureshi PPRA Advisor HEC

Grand Total Rupees (in words) FIVE MILLION, NINE HUDRED AND EIGHTY FOUR THOUSAND, FIVE HUNDRED AND FIFTY RUPEES ONLY.

MEMBER (EXTERNAL) CENTRAL PURCHASE COMMITTEE INSTITUTE OF BUSINESS ADMINISTRATION KARACHI

30/6/2021 Mabrook Khan Admin Officer CMB/UBK

MEMBER CENTRAL PURCHASE COMMITTEE INSTITUTE OF BUSINESS ADMINISTRATION KARACHI

Wajeeh Zaidi Sr. Manager IT IBA, Karachi

CHAIRPERSON CENTRAL PURCHASE COMMITTEE INSTITUTE OF BUSINESS ADMINISTRATION KARACHI

Dr. Sm Faisal Irfaat Assistant Professor Karachi

MEMBER CENTRAL PURCHASE COMMITTEE INSTITUTE OF BUSINESS ADMINISTRATION KARACHI

Syed Asghar Hussain Kazmi

Stamp & Signature