6. Technical Specifications & BOQ:

Scope of Services

(a) End to end deployment of the procured product.
(b) The necessary service support should be provided by Bidder during the agreement period.
(c) Training of two IBA resources on the purchased product from OEM authorized training Center.
(d) 3 years' comprehensive onsite warranty including maintenance.
(e) 24x7 on-site support with 2 hrs. Initial response time & 4 hrs. turnaround time

Architectural and Deployment Requirements

IBA is looking for a Unified Security Management solution, with below features and set of capabilities.

The solution should be based on "on premises" virtual environment, and not on any cloud based platform
The solution offered should be OPEX based model and not CAPEX based solution.
The unified pricing (on monthly subscription) basis, should be for unlimited number of Assets (Unique IP Address), and Not based on any EPS (Events per second), or TPS (Transaction per second).
Should have a distributed mode of deployment options with localized asset scanning, device event collection, vulnerability scanning features combined in remote probe/sensor for remote branches with integration on centralized management server

1. Software Solution

Sr. No.	Requirements	Bidder's Assessment (Y/N)
1	Solution Should support High availability and distributed environment that can show multiple sites threats in one GUI	Y
2	Solution should support multiple deployment options (on-premises, all-in-one appliances, virtual appliances)	Y
3	The solution architecture support heavy load from disparate IT assets for logs collection with no major performance degradation	Y
4	The solution must provide a mechanism for offline updates of software, signatures' and configuration information with minimal user intervention	Y
5	Ensure the integrity of the information collected from sources.	Y
6	Solution must and Integrated Threat Intelligence for events analyzing and correlation	Y
7	Provision of flexible and ease of integration, filtering, searching, correlation and analysis of events, logs or data across all distributed components.	Y

Stamp & Signature

MEMBER
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI
Syed Akbar Hussain Kazmi
Finance
IBA, Karachi

CHAIRPERSON
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI
DR. S.M. Faisal Inrodat
Assistant Professor
IBA, Karachi

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

8	The solution must supports file integrity monitoring for endpoints	Y
9	The solution must have capability of vulnerability scanning.	Y
10	The solution must have ability to identify network intrusions.	Y

2. Operational Requirements (Administration & Configuration)

Sr. No.	Requirements	Bidder's Assessment (Y/N)
1	Friendly and Ease of use interfaces (i.e. icons, menu bar, tips & help, drill downs, wizards etc.)	Y
2	Support both manual and automatic update of configuration information For example, security taxonomy updates, rule updates, device supported plugins, upgrades etc.	Y
3	Support protected web-based GUI to perform central management of all components, monitored assets, system administration, analysis and reporting tasks.	Y
4	Backup/recovery process for configuration.	Y
5	Real time dashboard of proposed system, security events, event category, network traffic etc. and notify the system administrator when problems arise.	Y
6	The solution must provide the ability to deliver multiple dashboards for management with security visibility.	Y
7	The solution deliver customizable dashboards (i.e. for Security Operation Center, threat management, compliance management, privileged users monitoring, monitored assets view, top security events view, network activities and attacks view)	Y
8	The solution support versatile and diversified built-in rules for policies / scenarios implementation	Y
9	The solution must provide the ability to store/retain both normalized and the original raw format of the event log for forensic purposes.	Y
10	The solution must provide the ability to normalize and aggregate event fields that are not represented by the out-of-the-box normalized fields.	Y
11	The solution is able to use the same management console to restore the archived logs to be re-processed, re-normalized and re-classified.	Y
12	The solution supports file integrity monitoring across monitored assets.	Y

MEMBER
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI
Syed Akbar Hussain Kazmi
Finance
IBA, Karachi

CHAIRPERSON
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI
Dr. S. M. Tousif Inadat
Assistant Professor
IBA, Karachi

MEMBER (EXTERNAL)
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI
Haris Qureshi
PPRA Advisor
HEC

Stamp & Signature

3. Logs/Events/Use Management Requirements

- OEM should give way forward for unsupported log source or application without any cost

Sr. No.	Requirements	Bidder's Assessment (Y/N)
1	Log collection that supports both short-term (online) and long-term (offline) event storage.	Y
2	The solution must support Industry log collection methods	Y
3	The solution provides agent-less collection of event logs whenever possible.	Y
4	The solution must normalize common event fields (i.e. username, IP addresses, hostnames, and log source device, etc.) from disparate devices across a multi-vendor network.	Y
5	The solution supports built-in use cases as per threat detection, network & application behavioral analysis, incident etc.	Y
6	The solution must provide long term trend analysis of events	Y
7	The solution normalizes common event fields (i.e. usernames, IP addresses, hostnames, log source device, commands, time and date stamping etc.) from disparate devices across a multi-OEM network. Specialized parsing/normalization requirements also be supported.	Y
8	The solution provides GUIs and wizards for to support the integration of unsupported data sources.	Y
9	The solution provides common taxonomy /categories of events.	Y
10	The solution provides the ability to store/retain both normalized and the original raw format of the event log for forensic purposes.	Y
11	The solution provides the ability to normalize and aggregate event fields.	Y
12	The solution supports the collector/agent send the log over TCP and encrypted from remote locations or secure zone.	Y

MEMBER (EXTERNAL)
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
Haris Kamran
PPRA Advisor
HEJ

MEMBER
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI
Syed Akbar Hussain Kazmi
Finance
IBA, Karachi

CHAIRPERSON
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI
DR. S. M. Faisal Iradat
Assistant Professor
IBA, Karachi

SUPERNET LIMITED Karachi

Stamp & Signature

Institute of Business Administration Karachi

4. Security Intelligence (Real-time monitoring, Event Correlation, Analytics and Alerting / Alarms)

Sr. No.	Requirements	Bidder's Assessment (Y/N)
1	The solution support and provide real-time monitoring of users and data access, intrusion, threats and attacks detection, behavioral profiling, suspicious/malicious activities, malware/virus proliferation, affected/compromised hosts, use cases anomalies, monitored assets anomalies, IPs and hostnames reputation, geo locations sessions, advanced persistent threats etc.	Y
2	The solution provides alerting based on observed security events, threats, indicators of compromise from monitored devices.	Y
3	The solution provides the ability to correlate information across potentially disparate devices.	Y
4	The solution should support a distributed database for event and network activity collection such that all information can be accessed from a single UI	Y
5	The solution should support a distributed database for event and network activity collection such that all information can be accessed from a single UI	Y

5. Advanced Threat Exchange

Sr. No.	Requirements	Bidder's Assessment (Y/N)
1	The solution supports and provides threat exchange feeds	Y
2	The solution allows integration with the threat exchange feeds and provide real time visibility of global threat landscape automatically as per critical and severity ratings of threat.	Y
4	The solution must support the ability to correlate against 3rd party security data feeds (geographic mapping, known botnet channels, known hostile networks, etc.). These 3rd party data feeds should be updated automatically by the solution.	Y
5	The solution supports IP and domain reputation, geo-location monitoring.	Y
6	The solution should dynamically learn behavioral norms and expose changes as they occur.	Y

MEMBER (EXTERNAL)
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI
Haris Qureshi
PPRA Advisor
HEC

Stamp & Signature

MEMBER
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI
Syed Akbar Hussain Kazmi
Finance
IBA, Karachi

CHAIRPERSON
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI
Dr. S M Faisal Iradat
Assistant Professor
IBA, Karachi

6. Database Security Events and Application Monitoring

Sr. No.	Requirements	Bidder's Assessment (Y/N)
1	User based activity analysis support	Y
2	Support for auditing / monitoring of DBMS including session monitoring/analysis; the solution should be able to capture DB audit trail without enabling it on DB (bidder can offer SIEM solution along with some additional tool to meet this requirement)	Y
3	Support for Parsing of DBMS for security analysis	Y
4	Database audit trail's performance hit must be less than 6%	Y
5	Database audit logs should contain all information which is available in the standard audit trail logs of database	Y
6	Customized monitoring and analysis on DB	Y
7	Solution should be able to integrate with customized business critical systems (Logs parsing and reports configuration should be possible)	Y
8	GUI base event logs parsing for custom/non supported devices.	Y
9	Alert or block against rule violation on DB	Y
10	Device/system access monitoring and analysis	Y
11	Data monitoring (for access and other defined operations) and analysis.	Y
13	Ability to detect access and leakage of sensitive data	Y
14	Ability to detect policy violations as per defined rules	Y

MEMBER (EXTERNAL)
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI
Haris Qureshi
PIRA Advisor
HEC

MEMBER
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI
Syed Akbar Hussain Kazmi
Finance
IBA, Karachi

CHAIRPERSON
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI
Dr S.M. Faisal Inadat
Assistant Professor
IBA, Karachi

SUPERMITTED Karachi

Stamp & Signature

7. Reporting

Sr. No.	Requirements	Bidder's Assessment (Y/N)
1	The solution must support the ability to schedule reports.	Y
2	The solution must provide templates for the easy creation and delivery of reports at multiple levels ranging from operations to business issues.	Y
3	The solution should provide 'canned' out-of-the-box reports for typical business and operational Issues	Y
4	The solution should provide tanned' out-of-the-box reports for specific compliance regulations (PCI, SOX, FISMA) and control frameworks including (NIST, COBIT, ISO).	Y
5	The solution must support the automated distribution of reports.	Y
6	The solution must support the capability to provide historical trend reports.	Y

	One Time Charges for Deployment (OTC) If any	Monthly Recurring Charges (MRC)
Total (PKR)	917,106.00	418,271.00
SST	(@13%) 119,223.78	(@17%) 71,106.07
Total Amount	1,036,329.78	489,377.07
Grand Total per Annum	6,908,854.62	

YV

Grand Total Amount per Annum Rupees (in words) SIX MILLION NINE HUNDRED EIGHT THOUSAND EIGHT HUNDRED FIFTY FOUR & PAISA SIXTY TWO ONLY

SUPERINTENDENT Karachi

Stamp & Signature

MEMBER / EXTERNAL
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI
Haris Qureshi
PPRA Advisor
HEJ

MEMBER
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI
Syed Akbar Hussain Kazmi
Finance
IBA, Karachi

CHAIRPERSON
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI
DR. S M Faisal Israat
Assistant Professor
IBA, Karachi