Appendix 1A- Functional Specifications - Scoring Sheet

Instructions of Filling up of Appendix

BC	Description
S	Standard feature. Required features readily available and to be provided by the bidder. Available from Day 1
C	Customization required. Bidder will provide the customization within the stipulated date (as per the project timelines provided in the RFP)by NABFINS

Marks for specifications for will be allotted against the responses to each of the point mentioned as per the following marking pattern:

Requirement Category	Standard	Customised
Must Have	10	0
Good to Have	5	3

Sheets will be scored on S/C scoring pattern, as per the above table.

Each line item in the functional specifications mentioned in Appendix 1A carries 10 marks. The marks allotted to the responses of the Bidder by the NABFINS, would be reduced to a scale proportionate to the marks allocated for the functional evaluation.

Notes	
1	Bidder is expected to provide for all requirements irrespective of the functionality of the solution proposed. Hence the overall cost must include all the requirements where the rank provided is S or C
2	In case the Bidder fails to provide a " Bidder Compliance" against any of the line items the response would be considered as incomplete and may not be scored, at NABFINS's discretion
3	Bidder is expected to provide the response by filling up the columns "Bidder' Compliance (BC)" and "Bidder Remarks" only. Bidder is advised not to make any changes to any information on the RFP documents for example insert a row or delete a row or modify any other information like change the functionality required, etc.
4	Every requirement needs to be treated as an individual requirement and should not be clubbed with any other requirement and the Bidder needs to provide a "Bidder's Compliance" for that individual requirement, in case the Bidder clubs the requirements the response would be treated as incorrect .
5	The Evaluation Committee decided by the NABFINS would be marking this annexure already scored by the bidder and would be appropriately assigning the final marks. The NABFINS will have the discretion to change the marks against the Bidder's scored line item if the bidder/OEM is not able to showcase the same in Product walkthrough or Presentation.
6	The marks allotted to the responses of the Bidder by the NABFINS after carrying out the above steps would be reduced to a scale proportionate to the marks allocated for the functional & technical evaluation for the respective module.
7	Bidder to ensure that any part compliance or Remarks which is not aligned with the Requirement shall be treated as Non-Compliance for Scoring Purpose and may lead to disqualification of bidder at NABFINS discretion

S. No.	Functional Requirement	Must have/ Good to have	Compliance [Yes/ No]	Remarks
	A. Platform & Architecture			
SIEM_001	Cloud base Hosted Application	Must have		
SIEM_002	High Availability (HA) architecture	Must have		
SIEM_003	Disaster Recovery support	Must have		
SIEM_004	Multi-tenant capability	Good to have		
SIEM_005	Horizontal scalability	Must have		
SIEM_006	Availability SLA (99.9%+)	Must have		
	B. Log Collection			
SIEM_007	Syslog log collection	Must have		
SIEM_008	Windows Event Log collection	Must have		
SIEM_009	Linux/Unix log collection	Must have		
SIEM_010	Agentless log collection	Must have		
SIEM_011	Agent-based log collection	Must have		
SIEM_012	API-based integration	Must have		
SIEM_013	Database audit log collection	Must have		
SIEM_014	Cloud log ingestion (AWS, Azure,Zoho,GCP)	Must have		
SIEM_015	SAAS Vendor Infra (HSM,ADV,DB,IAM)	Must have		
SIEM_016	SaaS application log collection	Must have		
SIEM_017	Custom parser support	Must have		
	C. Log Processing			
SIEM_018	Log normalization	Must have		
SIEM_019	Event categorization	Must have		
SIEM_020	Real-time Log Monitoring and Live Event Streaming	Must have		
SIEM_021	Duplicate event suppression	Must have		
SIEM_022	Time synchronization handling	Must have		
SIEM_023	Data enrichment	Good to have		
SIEM_024	Tamper-Proof/Immutable Log Storage	Must have		
SIEM_025	Minimum 365-Day Online Log Retention	Must have		
SIEM_026	Log Integrity Verification	Must have		
SIEM_027	Log Compression and Optimization	Good to have		
	D. Correlation & Detection			
SIEM_028	Rule-based correlation	Must have		
SIEM_029	Behavioral analytics (UEBA)	Must have		
SIEM_030	MITRE ATT&CK mapping	Must have		
SIEM_031	IOC correlation	Must have		
SIEM_032	Threat intelligence integration	Must have		
SIEM_033	Risk-based alerting and Threat hunting	Must have		
SIEM_034	Machine Learning analytics	Must have		
SIEM_035	Out-of-the-box (OOTB) Security Use Cases and Detection Rules	Good to have		
SIEM_036	Custom Detection Rule Creation and Modification	Must have		
SIEM_037	Rule Lifecycle Management (Create, Modify, Disable, Version Control)	Must have		
SIEM_038	Brute Force Attack Detection	Must have		
SIEM_039	Malware/Ransomware Behavior Detection	Must have		
SIEM_040	Data Exfiltration Detection Use Cases	Must have		
SIEM_041	Insider Threat Detection Capability	Must have		
	E. Alert Management			
SIEM_042	Real-time Event Correlation and Alerting	Must have		
SIEM_043	Alert prioritization and Alert suppression	Must have		
SIEM_044	Alert Incident Creator	Must have		
SIEM_045	Alert deduplication	Must have		
SIEM_046	Email notifications	Must have		
SIEM_047	SMS/Teams/Slack notifications	Good to have		

S. No.	Functional Requirement	Must have/ Good to have	Compliance [Yes/ No]	Remarks
SIEM_048	Alert SLA tracking	Good to have		
SIEM_049	False Positive Management and Alert Tuning Capability	Must have		
	F. Dashboards & Reports			
SIEM_050	Report export (PDF/CSV/Excel)	Must have		
SIEM_051	SOC dashboard	Must have		
SIEM_052	Executive dashboard	Must have		
SIEM_053	Custom Compliance dashboard and Report	Must have		
SIEM_054	Advanced Search with Query Builder Capability	Must have		
SIEM_055	Real-time dashboard refresh	Must have		
SIEM_056	Interactive dashboards	Good to have		
SIEM_057	Scheduled Report Generation	Good to have		
	G. Incident Management			
SIEM_058	Incident creation	Must have		
SIEM_059	Ticketing integration	Must have		
SIEM_060	Root cause tracking,	Good to have		
SIEM_061	Playbook execution	Must have		
SIEM_062	Automated Incident Enrichment	Must have		
SIEM_063	Case Attachment and Evidence Upload Support	Good to have		
SIEM_064	Security Incident Workflow Customization	Good to have		
SIEM_065	Incident Severity Classification and Prioritization	Must have		
	H. Compliance			
SIEM_066	PCI DSS reports	Must have		
SIEM_067	ISO 27001 reports	Must have		
SIEM_068	RBI Cyber Security compliance reporting	Must have		
SIEM_069	CERT-In reporting support	Must have		
SIEM_070	Audit trail	Must have		
	I. Security			
SIEM_071	Role-Based Access Control (RBAC)	Must have		
SIEM_072	Password policy enforcement	Must have		
SIEM_073	SSO support	Must have		
SIEM_074	Encryption at rest	Must have		
SIEM_075	Encryption in transit	Must have		
SIEM_076	Tamper-proof log storage	Must have		
	J. Performance			
SIEM_077	High EPS handling	Must have		
SIEM_078	Fast search capability	Must have		
SIEM_079	Long-term log archival	Must have		
SIEM_080	Data compression and Query optimization	Must have		
	K. Administration			
SIEM_081	Health monitoring	Must have		
SIEM_082	License monitoring	Must have		
SIEM_083	Backup & Restore	Must have		
SIEM_084	Configuration version control	Good to have		
SIEM_085	Log Source Health Monitoring (Connectivity, Parsing Status, EPS Monitoring)	Must have		
	L. Integration			
SIEM_086	Active Directory / LDAP Integration	Must have		
SIEM_087	Cloud Platform Integration (AWS, Azure, GCP)	Must have		
SIEM_088	Cloud Storage Dumped Logs Integration	Must have		
SIEM_089	Firewall integration	Must have		
SIEM_090	Endpoint security integration and DLP integration	Must have		
SIEM_091	Vulnerability scanner integration	Must have		
SIEM_092	PIM and PAM integration	Good to have		

S. No.	Functional Requirement	Must have/ Good to have	Compliance [Yes/ No]	Remarks
SIEM_093	MAF and IAM integration	Must have		
SIEM_094	Endpoint Detection & Response (EDR) and XDR Integration	Must have		
SIEM_095	Email Security Gateway Integration	Must have		
SIEM_096	Network Security Device Integration (IDS/IPS, Firewall,Core switch, VPN)	Must have		
SIEM_097	Database Audit Log Integration	Must have		
SIEM_098	Integration with Open-Source Threat Intelligence (STIX/TAXII)	Must have		
SIEM_099	Automatic IOC Enrichment and Correlation	Must have		
SIEM_100	Applications Log Integration (WAF, API Gateway, Application)	Must have		
M. AI & Automation				
SIEM_101	AI-assisted investigation	Good to have		
SIEM_102	AI-generated incident summary	Good to have		
SIEM_103	Automated response recommendations	Good to have		
SIEM_104	AI false-positive reduction	Good to have		
SIEM_105	Natural Language Search Capability for Security Events	Good to have		
N. Operations				
SIEM_106	IOC Lifecycle Management (Create, Track, Expire, Whitelist/Blacklist)	Must have		
SIEM_107	Case management	Must have		
SIEM_108	Evidence management	Good to have		
SIEM_109	Analyst collaboration	Good to have		
SIEM_110	Threat Hunting Capabilities	Must have		
SIEM_111	Support for CERT-In,RBI Incident Reporting	Good to have		
SIEM_112	The SIEM solution should provide a user-friendly search interface for efficient querying, filtering, analysis, and report generation of security logs and events.	Must have		
SIEM_113	Audit Trail for All Administrative Activities	Must have		
SIEM_114	API Rate Limit Monitoring and Failure Detection	Good to have		
SIEM_115	Asset Discovery and Asset Inventory Integration	Must have		
SIEM_116	Automated Response Actions (Block IP, Disable User, Isolate Endpoint)	Good to have		
SIEM_117	Approval Workflow Before Automated Response Execution	Good to have		
SIEM_118	Threat Hunting Query Support (KQL/SPL/SQL-like Query Capability)	Must have		
SIEM_119	MITRE ATT&CK Technique Coverage Mapping Dashboard	Must have		
SIEM_120	Threat Intelligence Feed Management (Add/Delete/Update Feeds)	Must have		