COMPLIANCE SHEET: Renewal of SIEM Solution License

Bidder must fill in this sheet with attention, duly signed and stamped.

Sr #	SIEM Solution Technical/Functional Requirement	Vendor Compliance Yes/NO, or Exception(s) to be added
1	Instant Search: Applies instant multi-level filtering to filtered data.	
2	Raw Logs for Advance Searching	
3	It will provide Agent Details (Network Interfaces, Ports, Packages and Processes etc.)	
4	Remote Agent Deployment from SIEM	
5	Windows Event ID Tuning and Configuration - Group Based Event Tuning	
6	Rule Tuning to capture new attackers and/or optimization	
7	Data Retention and Index Health Management	
8	Theme Customizer - User can switch Theme of application i.e. light & dark	
9	User Groups to categorize users based on roles, department, or duties.	
10	Audit Logs to capture all actions of users	
11	Auto Asset Discovery for identification of Unknown Devices	
12	The platform must support manual backups as well as automated, time-based backups for data integrity and continuity.	
13	Compliance Module (NIST, HIPAA, PCI DSS, GDPR, ISO, SOC 2, ADSIC, CIS and NESA)	
14	CIS-CAT and Open SCAP integration (CIS Benchmarking)	
15	Compliance count in respective dashboard	
16	ISO-27001 Compliance	
17	Customizable Visualization Module	
18	Agent and Agentless dashboards	
19	Threat detection through MAP visualization along with attacking IPs	
20	Map chart integration in custom visualization	
21	Provision for customizable dashboard creation as per user profiles/privileges.	
22	No-Code Custom Dashboards	
23	Custom Queries based Dashboarding	
24	The platform must support on-demand generation of customized reports tailored to specific user requirements.	
25	The platform must support scheduled generation of customized reports at predefined intervals or times.	
26	The platform must support query-based generation of customized reports, allowing users to dynamically extract data.	
27	Desktop App for Windows	
28	USB Detection Logs in the Network	
29	SMTP Configuration	
30	SNMP Traps and Device NetFlow	
31	Slack and Telegram Integration	
32	Integration of SAP ERP logs and Custom Dashboards	
33	Cloud, Hybrid and on-prem deployment is supported.	
34	Cloud Integration with AWS, GCP and Azure	
35	Organization Risk Score or Security Posture or Internal Attack Surface Management dashboards.	
36	Email Alert Reporting with respect to Alert Severity	
37	Configure Email Alerts with Severity Level	
38	Notifications (In-App, via Mobile Apps, Email)	

39	In-App and Off-App releases must be available for SIEM	
40	Reports can be scheduled over different intervals.	
41	Reporting Module with CSV and PDF Reports	
42	Report Customization Module	
43	Automated reporting for various compliance standards, including ISO-27001, GDPR, HIPAA, PCI-DSS, and more	
44	PDF report download support for all tables	
45	Device Risk Score must be assigned to all devices (Endpoints, Firewall, Router and Switch)	
46	Task Management, Status and Priority can be added against each alert, Vulnerability	
47	GeoIP Location Tracking	
48	Threat Intel 1 – Abuse IP DB	
49	Threat Intel 2 - Abuse Finder	
50	Threat Intel 3 – Cyber Protect Threat Score	
51	Threat Intel 4 - DNS Looking Glass	
52	Threat Intel 5 – DShield	
53	Threat Intel 6 - Echo Trail	
54	Threat Intel 7 - Google Safe Browsing	
55	Threat Intel 8 - IP-API	
56	Threat Intel 9 - IP info	
57	Threat Intel 10- MISP	
58	Threat Intel 11 - Malware Bazaar	
59	Threat Intel 12 - Alien Vault	
60	Threat Intel 13 - Phishing Initiative	
61	Threat Intel 14 - Stop Forum Spam	
62	Threat Intel 15 - Team Cymru	
63	Threat Intel 16 - Threat Miner	
64	Threat Intel 17 - URLhaus	
65	Threat Intel 18 - URL Scan IO Scan	
66	Threat Intel 19 - URL Scan IO Search	
67	Threat Intel 20 - VirusTotal	
68	Threat Intel 21 - OpenCTI	
69	MITRE Tactics and Techniques Mapping with Alerts	
70	Threat Intelligence for IP, Hash, URL and Domain	
71	Collective Threat Score and IOC Score for each IOC	
72	Assigning IOCs to User	
73	APT group information in SIEM	
74	File Activity Monitoring Module to observe all CRUD activities	
75	Vulnerability Detection for Network Devices (Firewall, Router, Switches etc.)	
76	The platform must generate a report to mention vulnerabilities whose patches are available along with a fixed version for that package and OS.	
77	The platform must generate consolidated reports identifying hosts that require specific patches.	
78	SIEM must collect and process logs from various sources, including routers, switches, servers, firewalls, IDS/IPS, applications, databases, and endpoints.	
79	Advanced correlation capabilities for detecting complex attacks or suspicious activities.	