SL. No.	SIEM	Essential (E) / Preferable (P)	Compliance Yes/No	Remarks(Bidder's Offer). Please provide adequate reference to product manuals/ documentation to substantiate how the product confirms to each requirement.
1	The proposed solution should be an appliance or Software with a clear physical or logical separation of the collection module, logging module and co-relation module.	E		
2	The proposed solution licensing should be by the number of events per second.	E		
3	The proposed solution should support log collection, correlation and alerts for the number of devices /applications mentioned in scope of work.	E		
4	The proposed solution should be able to support automatic updates of configuration information with minimal user intervention. i.e. security updates, vendor rule updates, device integration support, etc.	P		
5	The proposed solution must ensure all the system components continue to operate when any other part of the system fails or loses connectivity.	E		
6	The proposed solution must have an automated backup/recovery process.	E		
7	The proposed solution must automate internal health checks and notify the user in case of problems.	P		
8	The proposed solution should be able to perform single site & multi-site correlation across the network.	E		
9	The proposed solution should provide collection of events through customization of connectors or similar integration for the assets that are not natively supported. They should adhere to industry standards for event collection : syslog, OPSEC, WMI, SDEE, ODBC, JDBC, FTP, SCP, HTTP, text file, CSV, XML file etc.	E		
10	The proposed solutions should be able to collect data from new devices added into the environment, without any disruption to the ongoing data collection.	E		
11	The proposed solution should have connectors to support the listed devices/ applications, wherever required the vendor should develop customized connectors at no extra cost	E		
12	In the proposed solution, all logs should be Authenticated (time-stamped across multiple time zones) encrypted and compressed before transmission.	E		
13	The proposed solution should be able to continue to collect log data during database backup, de-fragmentation and other management scenarios, without any disruption to service	E		
14	The proposed solution should provide options to load balance incoming logs to multiple collector instances.	P		
15	The proposed solution should support log collection from all operating systems and their versions including but not limited to Windows, AIX,Unix, Linux, Solaris servers etc.	E		
16	The proposed solution should be able to store/retain both the log meta data and the original raw message of the event log for forensic purposes.	E		
17	In case the connectivity with SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually.	P		
18	The proposed solution shall allow bandwidth management, rate limiting, at the log collector level.	P		
19	The proposed solution should ensure that the overall load on the network bandwidth at DC, WAN level is minimal	P		
20	The proposed solution should provide time based, criticality based store and forward feature at each log collection point	E		
21	The proposed solution should have the capability to compress the logs by at least 70 % for storage optimization.	E		
22	The proposed solution should be possible to store the event data in its original format in the central log storage	P		
23	The data archival should be configured to store information in tamper proof format and should comply with all the relevant regulations.	E		
24	Traceability of logs shall be maintained from the date of generation to the date of purging.	P		
25	The proposed solution must support log archives on 3rd party storage.	E		
26	The proposed system shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.	E		
27	The proposed solution should be feasible to extract raw logs from the SIEM and transfer to other systems as and when required.	E		
28	The proposed solution should support the following log collection protocols: Syslog over UDP / TCP, Syslog NG, SDEE, SNMP Version 2 & 3, ODBC, FTP, Windows Event Logging Protocol, Opsec,Netflow at a minimum.	E		
29	The proposed solution should provide mechanism that guarantee delivery of events to the log management system and that no events will get lost if log management system is unavailable	E		
30	The proposed solution should prevent tampering of any type of logs and log any attempts to tamper logs. It must provide encrypted transmission of log data to the log management.	E		
31	The proposed solution should allow the creation of an unlimited number of new correlation rules	E		
32	The proposed solution should be able to integrate with security and threat intelligence feeds data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.) for the purpose of correlating events. These data feeds should be updated automatically by The proposed solution.	E		
33	The proposed solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Historical based, Heuristics based, Behavioral based etc. , across potentially disparate devices.	E		
34	The proposed system/solution should have the ability to correlate all the fields in a log	E		
35	The proposed solution should be able to parse and correlate multi line logs	P		
36	The proposed solution should have the ability to gather information on real time threats and zero day attacks issued by anti-virus or IDS/ IPS vendors or audit logs and add this information as intelligence feed in to the SIEM solution via patches or live feeds	E		
37	The proposed solution should allow a wizard based interface for rule creation. The proposed solution should support logical operations and nested rules for creation of complex rules	E		
38	The central correlation engine database should be updated with real time security intelligence updates from OEM	E		
39	The dashboard should be in the form of a unified portal that can show correlated alerts/ events from multiple disparate sources such as security devices, network devices, enterprise management systems, servers, applications, databases, etc.	E		
40	Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users	E		
41	The dashboard should show the status of all the tools deployed as part of the SOC, including availability, bandwidth consumed, system resources consumed (including database usage)	P		
42	It should be possible to categorize events while archiving for example , events for network devices, antivirus, servers etc.	P		
43	Any failures of the event collection infrastructure must be detected and operations personnel must be notified as per SLA. The device Health monitoring must include the ability to validate that original event sources are still sending events	E		
44	The proposed solution should generate the following reports (but not restricted to): User activity reports, Configuration change reports, Incident tracking report, Attack source reports etc. In addition, The proposed solution should have a reporting writing tool for development of any ad-hoc reports.	E		
45	The Dashboard design for The proposed solution should be editable on an ad hoc basis as per the individual user need	P		
46	The proposed system should display all real time events. The proposed solution should have drill down functionality to view individual events from the dashboard	E		
47	The proposed solution should allow applying filters and sorting to query results.	E		
48	The proposed solution should allow creating and saving of ad hoc log queries on archived and retained logs. These queries should be able to use standard syntax such as wildcards and regular expressions.	E