The bidder must indicate its compliance / non-compliance to the requirements and should substantiate its response in the space provided below. If more space is required to justify compliance, please ensure that the substantiation is clearly cross-referenced to the relevant requirement.

1. TECHNICAL SOLUTION REQUIREMENTS

ADMINISTRATION REQUIREMENTS FUNCTIONALITY			
REQ#	Technical Requirements	Comply or Not Comply	Provide details of how your solution satisfies Sasria requirements
FRQ1	The solution must support auto discovery of assets that are being protected or monitored.		
FRQ2	The solution must support automated classification of assets that are being protected.		
FRQ3	The solution must provide an open API for access to data stored within different information database(s).		
FRQ4	The solution must provide the ability to encrypt communications between components.		
FRQ5	The Security Intelligence solution must provide central management of all components and administrative functions from a single web-based user interface.		
FRQ6	The solution must integrate with other security and network intelligence solutions. Describe the level of integration and solutions supported.		
FRQ7	The SIEM must leverage passive asset discovery to allow new or possibly unauthorized devices to be profiled and tracked without manually scanning the network.		
LOG MANAGEMENT AND EVENT ANALYSIS FUNTIONALITY			
REQ#	Technical Requirements	Comply or Not Comply	Provide details of how your solution satisfies Sasria requirements

FRQ8	The solution must have a log collection and archive architecture that supports both short-term (online) and long-term (offline) event storage. • Describe how your solution manage, store, and archive the log data.		
FRQ9	The solution must support industry log collection methods (syslog, WMI, JDBC, SNMP, Checkpoint LEA, etc.)?		
FRQ10	The solution must provide agent-less collection of event logs whenever possible.		
FRQ11	The SIEM must provide a simple architecture with a single appliance to collect logs and network flow data.		
FRQ12	The solution must normalize common event fields (i.e. usernames, IP addresses, hostnames, and log source device, etc.) from different devices across a multi-vendor network.		
FRQ13	The solution must provide the ability to store/retain both normalized and the original raw format of the event log for forensic purposes.		
FRQ14	The solution must provide the ability to normalize and aggregate event fields that are not represented by the out-of-the-box normalized fields.		
FRQ15	The SIEM must provide a real-time event view of monitored information in raw/original as well as processed/parsed format.		
FRQ16	The solution must provide near-real-time analysis as well as long-term trend analysis of events with advanced drill-down functionality.		
FRQ17	The solution must provide the ability to aggregate an analyse events based on a user specified filter.		
SECURITY INCIDENT AND EVENTS MONITORING FUNCTIONALITY			

REQ#	Technical Requirements	Comply or Not Comply	Provide details of how your solution satisfies Sasria requirements
FRQ18	The solution must provide the ability to correlate information across potentially disparate devices.		
FRQ19	The solution must provide alerting based on observed anomalies and behavioural changes in network activity (flow) data. • Describe any standard alerts and method for adding user-defined anomaly and behaviour alerts.		
FRQ20	The solution must provide the ability to transmit alerts using multiple protocols and mechanisms to other management solutions.		
FRQ21	The solution must limit the presentation of multiple similar alerts. • Describe the solutions ability to minimize duplicate alarms.		
FRQ22	The solution must support the ability to correlate against 3rd party security data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.) and vulnerability scan results. These 3rd party data feeds should be updated automatically by the solution.		
FRQ23	The solution must provide an out of the box mechanism to discover and classify assets by system type (i.e. mail servers vs. data base servers) to minimize false positives associated with poor asset classification.		
FRQ24	The SIEM must have the ability to correlate on both flows and events within one correlation rule, thus reducing the number of false positives.		
FRQ25	The SIEM must provide correlation in real time.		
NETWORK ACTIVITY FUNCTIONALITY			

REQ#	Technical Requirements	Comply or Not Comply	Provide details of how your solution satisfies Sasria requirements
FRQ26	The solution **must** be able to profile communication originating from or destined to the internet by Geographic regions in real-time.		
FRQ27	The solution **must** identify network traffic within a virtual network environment.		
FRQ28	The solution **must** support application definition beyond protocol and port. The system **must** support the identification of applications using ports other than the well-known, and applications tunnelling themselves on other ports (e.g., HTTP as transport for MS-Instant Messenger should be detected as Instant messenger - not HTTP).		
FRQ29	The solution **must** detect “zero-day” events.		
FRQ30	The solution **must** dynamically learn behavioural norms and expose changes as they occur. • Detail the methods used by the solution and the method by which anomalies are displayed.		
FRQ31	The solution **must** detect denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. • Describe how the solution detects and displays this information.		
THREAT MANAGEMENT			
REQ#	Technical Requirements	Comply or Not Comply	Provide details of how your solution satisfies Sasria requirements
FRQ32	The solution **must** provide the ability to contextually link reported security events with real-time knowledge of the assets that are being targeted.		
FRQ33	The solution **must** provide the ability to assign credibility ratings to monitored security devices.		

FRQ34	The solution **must** be able to automatically change the credibility weightings of security devices in response to network-wide attacks.		
FRQ35	The solution **must** provide ability to send notification of correlated alerts via well-defined methods (i.e. SNMP trap, email, etc.)?		
FRQ36	The solution **must** provide embedded workflow capability that security operations staff can use to guide their work?		
FRQ37	The solution **must** provide bi-directional integration with 3rd party trouble ticketing/help desk systems that security operations staff may use to guide their work?		
FRQ38	The solution **must** provide a mechanism to track security incidents across a wide range of relevant attributes (i.e. IP addresses, usernames, MAC address, log source, correlation rules, user defined, etc.). The user **must** be able to filter incidents with the defined attributes.		
OPERATIONAL REQUIREMENTS FUNCTIONALITY			
REQ#	Technical Requirements	Comply or Not Comply	Provide details of how your solution satisfies Sasria requirements
FRQ39	The solution **must** provide the ability to deliver multiple dashboards that can be customized to meet the specific requirements of different users of the system.		
FRQ40	The solution **must** deliver sample dashboards out of the box (i.e. for threat management, compliance management, etc.).		
FRQ41	The solution **must** maintain a database of all assets discovered on the network. This asset data must include important information about the asset as learned by the information collected (i.e. system attributes, network attributes, vulnerability state, etc.). The database must provide the ability to edit attributes when they cannot be		

	learned (i.e. department, location, etc.). The user must be able to search this database.		
FRQ42	The solution must support multiple display points in different locations. Sasria needs to have the same visibility as the SOC.		

2. NON-FUNCTIONAL REQUIREMENTS

OPERATIONAL				
REF#	Item	Description	Comply or Not Comply	Comment
NFR1	Accessibility	System should be accessible using Desktop and Mobile devices using network cable, WIFI and/or 3G/4G/5G		
NFR2	Response time ranges	Front-end / host / back end: max 15 seconds.		
SECURITY AND PRIVACY				
REF#	Item	Description	Comply or Not Comply	Comment
NFR3	Identification and authentication	Users must be assigned unique identities within the system, which clearly identifies who they are. The system must only be accessed by legitimate and authorised users		

		including users from external entities. The system must utilise username and password to authenticate users and support two-factor authentication to strengthen access control when necessary.		
NFR4	User Group Definitions	Role-based access control shall be used to define content and functionality applicable to users. This must be in line with the user's job function or role. Departments will define access rights and the SIEM system administrator with permission from respective departments can only edit these access rights. Segregation of duties rules must be enforced on a system level.		
NFR5	Database Security	The database must be secured by allowing only authenticated and authorised users access to data. The database must be secured by only allowing the Web applications to access data through a service account, which forms part of Windows authentication.		

NFR6	Confidentiality	Data must only be accessed by authenticated and authorised users in line with their job function or role. Data and Passwords must never be viewable at the point of entry or at any other time during the SIEM processes lifecycle.		
NFR7	Data Loss (Disclosure of information about individuals or entities)	Security policies must be enabled to prevent leakage/disclosure of sensitive information to unauthorised users. Users must be trained on the functionality of the system to understand their responsibilities to safeguard sensitive information.		
NFR8	Data Encryption	All data flowing within internal and external SIEM modules must be encrypted with the latest industry standard encryption technology. All data utilised within the SIEM system must be encrypted when in storage, or in transit.		
NFR9	Data Integrity (Data Corruption)	All the information flowing within and across the SIEM modules should be the same and not be altered throughout its lifecycle. The information must not be compromised during changes and		

		must still be intact after the changes or updates to the SIEM system. Only authorised users must be able to edit or make changes to data.		
NFR10	Access Reports	Reports on user access and activities must be available to monitor policy violations.		
AUDIT TRAIL				
REF#	Item	Description	Comply or Not Comply	Comment
NFR11	Audit trail	Enable transparent audit trail in the system, audit trails must be created for all user actions that are performed. The following information will be recorded in the audit log: • User name • Date and time of action • Field name • Before value • After value • Effective date • Source (Direct/Web) The audit logs are stored in a separate database		
RELIABILITY				

REF#	Item	Description	Comply or Not Comply	Comment
NFR12	The system must be available 99% - 100% of its lifespan.			