ANNEXURE 3 A – MANDATORY SERVICE AND SOLUTIONS COMPLIANCE REQUIREMENTS - MANAGED SECURITY SERVICES AND SIEM SOLUTION

Meeting all requirements in Annexure 3 A are mandatory and Bidders must sign the necessary sections to indicate and confirm their contractual obligation to provide these services and features at the time the bid is awarded.

Failure to meet all requirements or signing the required sections where indicated will result in the submission being disqualified.

A.1 - Project Initiation Commitment

	Requirement	Comply (Y/N)
A.1.1	Prior to commencing the monitoring services, the Bidder must perform an assessment of PRASA's cybersecurity detection and prevention capabilities, recommend improvements and assist with implementation strategies.	

Signature: _____

A.2 - SIEM Capabilities

	Requirement	Comply (Y/N)
A.2.1	**Real time ingestion.** The solution will have the ability to ingest logs in real or near real-time and allow for instant searching.	
A.2.2	**Data Correlation.** The SIEM will have the ability to ingest logs and correlate it with threat intelligence feeds to identify malicious activity or indicators of compromise.	
A.2.3	**Real-time alerting.** The solution will have the ability to alert analysts and first responders as critical events of interest are	

	detected. Alert integration must include at a minimum email, WhatsApp and Telegram.	
A.2.4	**Use cases.** The SIEM solution must have predefined and common use cases ready to use. The SIEM must also have a capability to allow for custom use cases to be written and deployed by PRASA.	
A.2.5	**Coverage.** The solution must have the ability to consume log events using the Common Event Format (CEF) or known technology log formats without additional ETL processes. Where CEF is not possible, the solution should allow for custom ingestion scripts. As a minimum, the SIEM solution must be able to integrate from the following sources: C.2.5.1 - Windows, Linux and Unix type event logs C.2.5.2 - Network management and routing devices and appliances C.2.5.3 - Anti-virus, anti-malware, security auditing software, vulnerability management technologies and identity and access management logs. C.2.5.4 - For maximum effectiveness, the SIEM must be able to integrate with customized data sources and feeds, such as legacy applications to homegrown databases. C.2.5.5 - Database logs such as Microsoft SQL, Oracle and SAP. C.2.5.6 – Application logs such as SAP. C.2.5.7 - Networking and perimeter security appliances such as CISCO.	
A.2.6	**Data retention.** Logs must be kept for a period of 18 months and the platform must be able to assist with retention management. - Data required for immediate searching should be in a hot state for 30 days. - Data that is older than 30 days should be kept in a warm state for 90 days. - Data older than 90 days must be archived or snapshot, however, it must still be searchable.	
A.2.7	**Dashboards.** The SIEM solution must have pre-built dashboards for known and common activity reporting use cases, as well as the ability for custom dashboards to be created.	
A.2.8	**Data enrichment.** The SIEM integration capability must allow for data enrichment at the time of data collection but prior to data ingestion into the SIEM data set. An example is enriching web server event logs where IP addresses are immediately mapped according to geolocation tagging.	

A.2.9	**Analytics.** The solution must provide an analytics interface in which events can be searched or displayed in a timeline format. The interface must allow for search queries based on an open search query language and regular expressions.	
A.2.10	**MITRE ATT&CK Integration.** The solution must be able to align its threat detection indicators to the MITRE ATT&CK framework.	
A.2.11	**Machine Learning.** The solution must have the ability to perform anomaly detection based on machine learning techniques (UEBA).	
A.2.12	**Investigation Workspace.** The solution must have a built-in incident case management system that will generate incident investigation tickets and case management processes. The workspace should include a security workflow that will allows analysts to visualize the security monitoring stages, the incident response process, and the events that occur across each of these stages.	

Signature: _____

A.3 - Service Provider Capabilities

	Requirement	Comply (Y/N)
A.3.1	**24\7 Security monitoring.** The Bidder must have the ability to provide a 24x7 event monitoring and alerting function.	
A.3.2	**Proactive threat hunting.** The Bidder must not just rely on known indicators and use cases found in the SIEM technology but must also be able to perform continuous threat hunting using behaviour analytics and security intelligence.	
A.3.3	**Integrated incident response.** The Bidder must have the ability to work with PRASA to isolate and contain an incident and provide virtual or onsite assistance to high priority events.	
A.3.4	**Fast and agile deployment.** The Bidder must be able to rapidly deploy their solution in a hybrid environment scenario, i.e., on-premises as well as cloud environments. Bidders must detail how they will implement an event logging and SIEM capability (where cloud and on-premises logs are collected and correlated) providing PRASA with a single pane of glass across both environments.	
A.3.5	**Up to the minute security intelligence (APT analysis).** The Bidder must be able to utilise a broad range of threat intelligence feeds together with in-house research to construct insights in line with PRASA's industry.	
A.3.6	**Offensive security insight.** The Bidder must be mindful around the tactics, techniques and processes used by both Attackers and Defenders (Purple Teaming) as part of their capability offering.	
A.3.7	**Incident forensics.** Where an incident is identified that warrants a serious investigation, the Bidder must be able to initiate incident forensic procedures to secure the necessary evidence, in line with South African regulatory requirements.	
A.3.8	**Incident playbooks.** The Bidder must be able to generate and design specific incident response playbooks in line with the threat model for PRASA.	
A.3.9	**Reporting matrix and KPIs.** The Bidder must be able to provide a reporting matrix and key performance indicator to demonstrate the Bidder's performance at defined intervals providing the service.	
A.3.10	**Cyberthreats countermeasures planning through research and development.** The Bidder must provide PRASA with relevant cyber security research and industry specific cyber tendencies which could help PRASA prepare for current or future threats.	
A.3.11	**Vulnerability identification and remediation.** Apart from log and event monitoring, the Bidder must have the ability to continuously scan the PRASA environment (internally and externally) for infrastructure and software vulnerabilities. The	

	results of these scans must be included in the monitoring capabilities.	

Signature: _____

A.4 - Solution Architecture Components

The solution design and architecture must include the following non-functional requirements in the design.

	Requirement	Comply (Y/N)
A.4.1	**Location –** The SIEM must be implemented on-premises. Components that need to be cloud based, must reside in the geographical borders of South Africa.	
A.4.2	**High Availability (HA)** – The Bidder's solution must be able to recover from failure without causing the loss of data consumption or services.	
A.4.3	**Scalability** – The Bidder's solution must be able to scale, either through horizonal or vertical improvements to the stack.	
A.4.4	**Security** – The Bidder must offer a solution that is secure and can be integrated with PRASA's existing identity and access management capabilities.	
A.4.5	**Maintainability**: The Bidder should offer a solution that is easy to maintain & support with the capability to make modifications without affecting service.	

This is to certify that the Bidder has / have acquainted himself / themselves with the General Compliance Requirements in the tables above for the Managed Security and SIEM tender and accepts/commits to the requirements.

THUS DONE and SIGNED at _____

Signature: _____

on this _____ day of _____

DULY AUTHORISED SIGNATORY(IES) WITNESSES

1. _____ 2. _____