

No.	Bidders' Queries	SANParks Response
1	Are you looking for a full SIEM or only Log Management?	Log Management
2	What is the Data retention requirement for online and archive logs?	90 Days
3	Are you okay with SAAS Platform in running in a public cloud?	Cloud Based
4	Can you share volume of logs that will be ingested per day or the events per second requirement	
5	Any specific outcome that needs to be achieved as part of the product?	Needs to meet tender requirements
6	What use cases need to be deployed?	As per tender requirements
7	For the log sources shared in scope, can you provide the following information?	See table below
8	How many instances of Microsoft SQL are there in scope for this bid?	34
9	How many Azure AD/EntraID tenants are there?	1
10	How many MYSQL instances are there?	3
11	How many Progress SQL instances are there?	3
12	For SAGE People, Online Bookings, MS Great Plains, Roomseeker, GTPMS and CRM, are we just collecting logs from the applications and not the server running them as well? If servers are in scope, please list how many servers and their OS	No Server in scope
13	What is the estimated daily log volume (in GB) that SANParks currently generates across all systems, and what is the projected growth over the five-year contract period?	See below table
14	Are all six SANParks regions (Arid, Cape, Garden Route, Frontier, North, and Kruger National Park with 35 camps) connected via a central network, or will the log management solution need to accommodate multiple isolated networks?	Via a central network

	Context: Network topology affects architecture design and bandwidth requirements.	
15	Does SANParks have a preference for cloud-based (SaaS), on-premise, or hybrid deployment of the log management solution? Context: This affects solution selection, data sovereignty, and infrastructure requirements.	Cloud based
16	What is the current network bandwidth available between the Head Office in Pretoria and the various regional offices and camps? Context: Bandwidth constraints may impact log transmission strategies and require local collectors.	300mbps
17	For the Linux CentOS 7 systems mentioned, is SANParks planning to upgrade these systems given CentOS 7 end-of-life status, and should the solution accommodate migration to alternative distributions? Context: This affects long-term compatibility and support planning.	No. The upgrade or deployment of an alternative Server OS is defined and restricted by the fact that it needs to support legacy PHP5.6 for example.
18	What are the specific availability requirements (e.g., 99.9%, 99.99%) for the log management solution? Context: SLA requirements impact architecture design and pricing.	99.9
19	What is the required log retention period for different types of logs (security, application, system), and are there specific compliance requirements driving these retention periods?	90 Days

	Context: Storage sizing and compliance feature requirements depend on retention policies	
20	What is the maximum acceptable latency for real-time alerts on critical security events? Context: This determines whether edge processing capabilities are required	60 seconds
21	How many concurrent users are expected to access the log management system, and what are their typical use cases (security analysis, compliance reporting, troubleshooting)? Context: User licensing and performance requirements	5 Users
22	Does SANParks currently have any SIEM, log management, or monitoring tools in place that the new solution must integrate with or replace? Context: Integration requirements and migration planning	SIEM, Yes
23	For the Progress SQL (Linux Environment) and GTPMS systems, can you provide more details about these applications and their log formats? Context: Custom connector development may be required for proprietary systems	OK some corrections: This I guess would be Postgres SQL server (not Progress). Also we use MySQL. These are not application as such, rather the website logs actions in our (for example) Reservations web interface. The logs can be bespoke and adjusted to requirements. Some examples will be: - Log every action on the website for a reservation: I added a unit on the Reservation detail page (log it), I added items to the basket page (log it), I clicked on Checkout to get my final Quote (how much to pay for what) – Log it.

		- I made a payment – Log the amount and outcome of payment – Settled/Failed etc... Log it - Keep record of all payment transactions in an audit table... Log it. It captures actions performed by a customer on one of our systems) – such as Reservations, Quick Pay, Travel Trade. It is part of a page on the web or an action on the web... you click on the button Checkout on your reservation, then log it. You start a payment (checkout pre-payment) (log it), your payment was processed and Settled (log it) you change your reservation nights (log it)
24	Are there any specific Microsoft 365 or Azure services beyond Azure AD/Microsoft Entra that require log collection (e.g., Exchange Online, SharePoint, Teams)? Context: Identifying potential integration complexities early	No
25	For the software licensing component, would SANParks prefer a perpetual license model with annual maintenance or a subscription-based model? Context: Different vendors offer different licensing models affecting cash flow and TCO.	Please price as per provided pricing model in the tender document.
26		

	Should the pricing include any hardware components if an on-premise solution is proposed, or will SANParks provide the necessary infrastructure?	
	Context: Clarifies scope of supply and pricing boundaries.	All inclusive pricing as per tender requirements
27	For annual price escalations in years 2-5, should bidders use a specific CPI baseline, or will the actual CPI at the time of escalation be applied? Context: Pricing predictability and contract terms	Inclusive pricing as per tender requirements
28	Are there any volume-based pricing considerations if log volumes exceed initial estimates? Context: Ensures pricing model accommodates growth.	No just price as per pricing model
29	Regarding the performance security requirement, what percentage of the contract value is required, and in what form (bank guarantee, surety, etc.)? Context: Financial planning for contract execution	Will form part of contracting negotiations with successful bidder.

30	Will SANParks accept a phased payment structure aligned with implementation milestones rather than upfront payment for licenses? Context: Cash flow management and risk mitigation	Please price as per SBD 3.1 in the tender document
31	In case of technology obsolescence during the five-year period, would SANParks consider provisions for technology refresh or solution upgrades? Context: Long-term solution viability and innovation	As SDB 3.1 support and maintenance is required for the 5 years
32	Should the support and maintenance services include 24/7 monitoring and incident response, or only technical support for the platform? Context: Determines whether managed SOC services should be included	All inclusive as per SBD 3.1
33	Are there any specific service level penalties or remedies expected beyond those outlined in the General Conditions of Contract? Context: Risk assessment and pricing considerations	No

34	Should the solution include any professional services for use case development, correlation rule tuning, or threat hunting beyond initial implementation? Context: Ongoing professional services requirements.	Fully functional solution to meet tender requirement
35	What are SANParks' preferred support hours (business hours only vs 24/7), and should support be provided on-site, remotely, or hybrid? Context: Support model design and resource planning.	Business hours/remotely
36	Does SANParks require dedicated support resources, or is a shared support model acceptable? Context: Resource allocation and pricing model.	No dedicated support resources
37	What is the expected response time for different severity levels of incidents (Critical, High, Medium, Low)? Context: SLA definition and support team sizing.	Response to incidents out of scope
38	Will SANParks provide dedicated resources for the implementation project, including project management, technical, and business stakeholders? Context: Implementation planning and resource coordination.	No

39	Are there any planned ICT infrastructure changes or upgrades during the implementation period that might affect the project timeline? Context: Risk identification and timeline planning	No
40	Can implementation activities be performed during business hours, or will after-hours/weekend work be required to minimise disruption? Context: Resource planning and potential additional costs	During business hours
41	Is there a preferred sequence for rolling out the solution across regions, or should all locations be implemented simultaneously? Context: Phased vs big-bang implementation approach	No regional implementation
42	What is the expected frequency for system health checks, performance reviews, and service review meetings? Context: Operational Governance Planning	Monthly
43	Should the solution include automated compliance reporting for specific frameworks (POPIA, GDPR, PCI-DSS, etc.)? Context: Compliance feature requirements	Yes as outlined on the bid document
44	What are the backup and disaster recovery requirements for the log data?	Back up and DR out of scope and will be done in terms of SANParks policy.

	Context: Business continuity planning and architecture design	
45	For the reference letters requirement, would SANParks accept references from implementations done through partners or must they be direct client engagements? Context: Reference letter preparation	As outlined on the bid document
46	Can international reference letters be submitted if they meet all other requirements? Context: Leveraging global experience and references	As outlined on the bid document
47	For the solution design document, is there a page limit or specific format requirement? Context: Document preparation guidelines	No
48	What is the expected duration of the presentation session, and how many SANParks stakeholders will participate? Context: Presentation planning and preparation.	Will be determined and communicated with bidders who meet the stage requirements
49	Will SANParks provide access to a test environment for proof-of-concept during the evaluation process? Context: Demonstration of actual integration capabilities	No Sample/demo data is acceptable
50	Should the training for five SANParks personnel be conducted on-site at SANParks facilities, at the vendor's training facility, or online? Training logistics and cost planning.	Online
51	What is the expected skill level of the personnel to be trained (basic users, administrators, security analysts)?	Security analysts

	Context: Training curriculum development.	
52	Should the training include certification preparation for any vendor-specific certifications? Context: Value-added training offerings.	No
53	Is ongoing training for new staff members during the five-year period required, or only initial training for five personnel? Context: Long-term knowledge transfer planning.	Only 5 Personnel
54	Are there any specific encryption standards or algorithms required beyond "strong encryption algorithms"? Context: Technical security requirements.	No
55	Should the solution include specific features for insider threat detection or privileged user monitoring? Context: Advanced security use cases.	No
56	What are the authentication requirements for accessing the log management system (e.g., multi-factor authentication, integration with Active Directory)? Context: Access control implementation.	Integration with AD
57	SANParks anticipate any significant expansion of ICT infrastructure or new system deployments during the five-year contract period? Context: Scalability planning.	No
58	Is there an expectation for the solution to evolve to include SOAR (Security Orchestration, Automation, and Response) capabilities? Context: Future roadmap alignment.	No

59	Given the remote location of some parks, are there any special considerations for sites with limited or unreliable connectivity? Context: Edge deployment and offline capabilities.	No
60	What level of documentation is expected (user manuals, administration guides, architecture documents, runbooks)? Context: Documentation deliverables planning.	No
61	Should the solution include a knowledge base or self-service portal for SANParks users? Context: Additional value-added services.	No

SANParks' Response will be highlighted in red on the below table:

Log Source	Vendor	Expected Log Volume (GB Per day or Events per second)	Retention Requirement Online & Archive (In Days / Years)	Application Functionality (Identity, HRMS, Database, ERP etc)	Application Functionality (Identity, HRMS, Database, ERP etc)	Onprem or Cloud Hosted or SAAS?)	What are the use cases that need to be implemented? (Suspicious Activities, Logins, DB Activities etc)	Log Format (CEF, JSON, KVP, CSV, DB)	Type of Events to be Collected (Logins, Security, Config etc)
MS SQL Database	Microsoft	50GB	90 Days						
SAGE People		50GB	90 Days						

Online Bookings (Linux CentOS 7)		Out of scope	90 Days						
MICROSOFT GREAT PLAINS		50GB	90 Days						
ROOMSEEKER		50GB	90 Days						
AZURE AD/MICROSOFT ENTRA	Microsoft	Out of Scope	90 Days	Identity Datastore	API	SAAS		JSON	Admin, Audit, SignOn Events
DATABASE – MYSQL		50GB	90 Days						
Postgres SQL (Linux Environment)		50GB	90 Days						
GTPMS		50GB	90 Days						
CUSTOMER RELATIONSHIP MANAGEMENT (CRM)		50GB	90 Days						