Q&As for Cyber Security Management Services: SACAA/CSMS/00006/2026 - 2027

1. Please provide the current number of endpoints (750), servers (90), users (750), email mailboxes (850), identities (750), network devices (150), Azure subscriptions (2), and cloud workloads (50) that fall within the monitoring scope.
2. Please provide SACAA's current average and peak log-ingestion volume in GB or TB per month. 700GB per month
3. Please specify if there is a quantity of additional Trend Vision One ingestion credits and retention credits that bidders must include in pricing. 33767
4. Please confirm whether the six-month retention requirement applies to all raw logs and whether the data must remain immediately searchable within Trend Vision One. remain immediately searchable within Trend Vision One
5. Please provide a complete list of the Trend Micro Vision One modules, licences and subscriptions currently deployed, together with their quantities and expiry dates. This information will be provided during the contracting phase.
6. Please confirm whether bidders must renew or supply the existing Trend Micro licences, or only provide the additional ingestion and retention credits. only provide the additional ingestion and retention credits
7. Please confirm whether all existing sensors, connectors and log sources are already deployed and healthy, or whether onboarding, remediation and configuration work must be included. all existing sensors, connectors and log sources are already deployed and healthy
8. Please clarify whether the requirement for South African-based personnel applies only to Trend Vision One platform administrators, or also to all MDR analysts, threat hunters and incident-response personnel. ALL
9. Please confirm whether a shared 24/7 MDR team is acceptable or whether SACAA requires a dedicated team and dedicated shift roster. shared 24/7 MDR team is acceptable
10. Please specify the required acknowledgement, notification, investigation, containment and resolution SLA for Priority 1 to Priority 5 incidents.

Incident SLA Definitions (P1–P5)

Priority 1 – Critical (Business Down / Major Outage)

- **Acknowledgement:** 15 minutes
- **Notification:** 15–30 minutes (immediate escalation to stakeholders)
- **Investigation Start:** Within 15 minutes
- **Containment:** Within 1 hour
- **Resolution Target:** 4–8 hours (or workaround within 1 hour if full fix not possible)

Priority 2 – High (Severe Impact / Major Function Degraded)

- **Acknowledgement:** 30 minutes
- **Notification:** Within 1 hour
- **Investigation Start:** Within 30 minutes
- **Containment:** Within 2–4 hours
- **Resolution Target:** 1–2 business days

Priority 3 – Medium (Partial Impact / Non-Critical Business Disruption)

- **Acknowledgement:** 4 hours
- **Notification:** Within 4–8 hours
- **Investigation Start:** Within 1 business day
- **Containment:** Within 1–2 business days (if applicable)
- **Resolution Target:** 3–5 business days

Priority 4 – Low (Minor Issue / Limited Impact)

- **Acknowledgement: 1 business day**
- **Notification: Within 1–2 business days (if escalation required)**
- **Investigation Start: Within 2 business days**

- **Containment: As required (usually not applicable)**
- **Resolution Target: 5–10 business days**

Priority 5 – Service Request / Cosmetic / Informational

- **Acknowledgement: 2 business days**
- **Notification: On request or if delay expected**
- **Investigation Start: Within 3–5 business days**
- **Containment: Not applicable**
- **Resolution Target: 10–15 business days (or according to request complexity)**

11. Please clarify whether the successful bidder may perform containment actions directly, such as endpoint isolation, email deletion and malicious-IP blocking, or whether SACAA approval must first be obtained. successful bidder may perform containment actions directly, such as endpoint isolation, email deletion and malicious-IP blocking
12. Please confirm whether onsite incident response is required, the required response time and whether a fixed number of onsite incident-response hours or callouts must be included in the price. Callout may be included
13. Please confirm whether digital forensics, forensic imaging, malware analysis and evidence chain-of-custody services are included in the scope. NO
14. Please confirm whether the successful bidder is responsible only for identifying CREM risks and recommending remediation or must also implement remediation activities. Must also implement remediation activities
15. Please provide the number of users that must be covered by monthly phishing simulations and quarterly security-awareness training. 750
16. Please provide the expected contract commencement date, transition period, incumbent handover arrangements and required operational go-live date. Upon conclusion of the tender process
17. Please confirm whether a parallel-run period with the incumbent service provider is required and whether this must be included in the bid price. No, only during the handover period
18. Please confirm whether annual price escalation is permitted and how variable log-ingestion or licence consumption above the initial baseline should be priced. Price escalation is NOT permitted
19. Please confirm whether travel, onsite support, after-hours work, public-holiday support and incident-response callouts must be included in the fixed three-year price. Yes

20. Total number of Users connecting to the network i.e. generating telemetry data to be monitored from log sources such as Endpoint, Network, Email, AD/Auth, Firewall, DNS etc. Number of software licenses for workstation software can be a good starting point Or the number of Users in Active Directory. Note some industries leverage shared devices / accounts. We need to count all users that connect to the network. 750

21. Site Details: Users Per site, Servers per site, Number and make of Firewall(s) per site, Internet Bandwidth per site (capture in the table below)

Site/Location	Local Internet Break-out. Yes/No	Users	Servers	Hypervizor	Firewall	Total Internet Mbps (Ingress + Egress)	Core Switch Make and Model that FW connects to?	Core switch media type E.g. 1GbE Copper, 10GbE fibre N

								ote: 1GbE copper is preferred as it is more cost-effective)
Head Office	Yes- Direct	750	90	This information will be provided during the contracting phase.	This information will be provided during the contracting phase.	1000Mbps	This information will be provided during the contracting phase.	This information will be provided during the contracting phase.

23. Details of Public Cloud Providers and Cloud services in use (Here we are concerned about the compute element)
- Public Cloud Provider(s): Azure
- Total Number of IaaS Servers (VM's): 50
- Total Number of Containers: 50
- Total Number of Functions: 25

24. Email and Collaboration SaaS Services:

- Total Number of Users using Office/M365 and license type: 750 , E5
- Total Number of Users using Google Workspace and license type: 0
- Total Number of Users using Box and License type: 0

25. Security Stack:
- Firewall: This information will be provided during the contracting phase.
- End Point Protection / End Point Detection: This information will be provided during the contracting phase.
- Security Services Edge (SSE): This information will be provided during the contracting phase.
- VPN: This information will be provided during the contracting phase.
- Email Security / Email Gateway: This information will be provided during the contracting phase.
- Proxy Server: This information will be provided during the contracting phase.
- Identity and Access Management: This information will be provided during the contracting phase.
- Multi-factor Authentication: This information will be provided during the contracting phase.

27. Oracle Licensing: Does your organisation currently hold active Oracle licenses that can be leveraged for this deployment, or should we factor new licensing into our commercial proposal?
No, we do not have existing Oracle license