

Q and A Pack

RAF 2026 00059: PROCUREMENT OF A THREAT DETECTION AND RESPONSE SERVICES FOR THE ROAD ACCIDENT FUND (RAF) FOR A PERIOD OF FIVE (5) YEARS.

EMPLOYER:	The Road Accident Fund ("RAF")
RFP NUMBER:	RAF/2026/00059
DESCRIPTION:	PROCUREMENT OF A THREAT DETECTION AND RESPONSE SERVICES FOR THE ROAD
DATE OF PUBLICATION:	10 September 2026
BID VALIDITY PERIOD:	90 days from the Bid Closing Date
BID CLOSING DATE:	09 October 2026
BID CLOSING TIME:	11h00
TENDERS MUST BE HAND DELIVERED OR COURIERED TO:	The Road Accident Fund (RAF) 420 Witch Hazel Avenue Eco Glades 2 Office Park, Block F (at reception) Attention: RAF's Representative mentioned below
RAF'S REPRESENTATIVE	Tshiamo Motitswe: e-mail Tshiamomo@raf.co.za

1. With reference to bid RAF/2026/00059, please confirm whether the required Threat Detection and Response service must be delivered using RAF's existing, RAF-owned Microsoft Sentinel environment as the primary TDR platform.

Answer: Yes

2. Please also confirm whether bidders are required to propose or supply any additional licensed TDR, SIEM, SOAR, XDR or case-management product, or whether any supplementary tools used by the bidder should be included as part of the managed service price.

Answer: This RFP is for Threat Detection and Response services on top of the RAF's existing Threat Detection and Response solutions. There are no expectations of license/subscription costs from bidder proposals.

3. Please clarify which Microsoft Sentinel and related Microsoft licensing and consumption costs will remain for RAF's account, given that section 4.3.1 excludes licensing costs.

Answer: Yes. Subscription/license costs as well as ingestion and retention costs will be for the RAF's account.

4. The total number of endpoints that require protection (workstations, laptops, mobile devices, etc.)

Answer: +- 4000 (no licenses/tools required by the RAF)

5. The number of servers (physical and virtual) in your environment?

Answer: +- 500 (no licenses/tools required by the RAF)

6. The size of your network infrastructure (number of network devices, switches, routers, etc.)

Answer: +- 200 (no licenses/tools required by the RAF)

7. An approximate count of users/employees within the organization

Answer: +- 3500 (no licenses/tools required by the RAF)

8. Any specialized systems or applications that would require specific security consideration

Answer: Integrations with various in-house applications and cloud-based applications, through a combination of API and traditional log collection, in addition to integrations listed in the RFB document.

9. As we understand it, the RFP is for the provision of a 24/7/365 Managed Security Operations Centre (SOC) operating on top of the customer's existing Microsoft Sentinel SIEM environment.

Could you please confirm whether the SOC service and all associated security data/logs are required to be hosted and processed within South Africa due to government data residency requirements?

Answer: The SOC must be hosted in South Africa.

10. Please find the attached spreadsheet and assist in completing the sizing tool so we can determine the exact EPS and FPM requirements for an **on-premises (customer-managed)** deployment.

Please find the **EPS & Flow Calculator** attached. Kindly fill in RAF environment details and return the completed spreadsheet to us. This will allow us to extract the calculated Events Per Second (EPS) and Flows Per Minute (FPM) needed to size the core QRadar components accurately.

In addition to the calculator, please provide feedback on the following operational and technical requirements:

- **Licensing & User Counts**

- **QRadar SOAR / Resilient Users:** How many users will be required for the Security Orchestration, Automation, and Response (SOAR) platform?

- **Infrastructure & Hosting Environment**

- Deployment Form Factor: Do you intend to host the environment on virtual infrastructure (e.g., VMware ESXi / KVM) or dedicated physical appliances?
 - Resource Reservations: If virtualized, can the host platform guarantee dedicated CPU, RAM reservations, and high-performance storage (SSD/NVMe with requisite IOPS)?
 - Network Topology: Will this be a single-site deployment, or are there remote/branch sites that require dedicated Event Collectors or Disconnected Log Collectors (DLCs)?
- **Data Retention & High Availability**
 - Active Data Retention: What is your required retention period for online, searchable logs (e.g., 30, 60, or 90 days)?
 - Cold Archiving: Are there compliance requirements for long-term off-site backup or raw data cold archiving?
 - High Availability (HA) & DR: Is High Availability (HA) required for the Console or Event Processors, or is a secondary Disaster Recovery (DR) site planned?

Answer: Please note that the RAF is not looking for a Threat Detection and Response Solution in this RFP but for a service provider to provide Threat Detection and Response Services on a RAF-deployed security monitoring platform. The requested sizing information requested below, therefore are not relevant to the RFP as they relate to a platform.