



**state security**

State Security Agency  
REPUBLIC OF SOUTH AFRICA

**INVITATION TO PROVIDE INFORMATION**

<b>Document No.</b>	SSA/23/2021-22	
<b>Description</b>	REQUEST FOR INFORMATION FOR THE PROCUREMENT OF A THREAT DETECTION AND THREAT HUNT TOOLS	
<b>Contact Person:</b>		
	Name:	Ms Matshidiso Gaba
	Email address:	matshidisog@ssa.gov.za
	Telephone No:	(012) 426 2138
<b>Closing time and date and venue</b>	Time and Date:	11:00 on the 02 December 2021 at SSA Headquarters Reception, Musanda Complex, R50 Delmas Road, Rietvlei, PRETORIA
	Condition	<b>Information received after the closing time and date are late and will as a rule not to be accepted for consideration</b>  Documents should be in a sealed envelope clearly marked with the above document number, description and State Security Agency.
<b>Delivery address and conditions for delivery of documents</b>	Delivery address:	SSA Headquarters Reception, Musanda Complex, R50 Delmas Road, Rietvlei, PRETORIA  <b>Service Providers must ensure that the bids are delivered timeously to the correct address. The bid box will be open from:</b> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Monday to Friday – 08h00 to 16h00



**state security**

State Security Agency  
REPUBLIC OF SOUTH AFRICA

## TERMS OF REFERENCE

### 1. INTRODUCTION

#### **Cyber Threat Detection and Threat Hunt solution**

The project team has a requirement and responsibility to review and enhance its cyber security capability, response and readiness through threat detection and threat hunting tactical capabilities.

Terms of reference to deliver a comprehensive cyber threat detection and cyber threat hunt solutions to assist in the capacitation of the environment, in order to provide continuous and on demand ICT Security Monitoring and Information Assurance services

### 2. EVALUATION CRITERIA

#### 2.1 **Service Providers will be subjected to scrutiny to check whether the proposals received are compliant to the requirements stipulated on paragraph 2.2 below.**

**The below requirements should be complied with in full for both the company and the system proposed and bidders who do not comply with the Terms of Reference will be disqualified**

#### 2.2 **Requirements**

##### 2.2.1 **Key Deliverables (Project)**

2.2.1.1 Service provider or cyber security vendor is required to deliver a successful implementation within a stipulated project plan due to the need for immediate interoperability between the key deliverables that will provide the maximum impact at the earliest opportunity and subsequent years.

2.2.1.2 Service provider or cyber security vendor must demonstrate the ability to implement, maintain and support the solution and must provide a reference/s of where the solution is deployed.



2.2.1.3 Where the service provider or cyber security vendor is not the OEM, a requirement to provide OEM details and assurance (verifiable proof) from the OEM as the capable and reputable reseller to provide maintenance, support and OEM training.

## 2.2.2 Required key deliverables are as follows (Service Provider):

2.2.2.1 The service provider must provide valid OEM Authorization Certification that includes licensing, installation, configuration, building of rules and optimization with preferably the highest level of product support given by OEM to the service provider.

2.2.2.2 The bidder has the option to provide information for either threat detection (Complete solution) or threat hunting (Complete solution), or for both threat detection and threat hunting.

2.2.2.3 Threat detection and threat hunting: Provide solutions that are aligned with market related business requirements and best practices in cyber threat detection and threat hunting, response capabilities and processes.

2.2.2.4 The bidder must be prepared to provide a live demonstration in South Africa to enable the client to evaluate the basic required capabilities of the proposed solution such as searching, customization and reporting.

2.2.2.5 The cyber threat detection and threat hunting consultant should be able to work alongside the tactical cyber threat intelligence consultancy to deliver enhanced, proactive threat detection and threat hunting options.

2.2.2.6 Training: Provide an appropriate package of dedicated training to enable the project team to optimally derive value out of the required tools. The successful vendor should also clearly demonstrate a plan to mature and transfer Mission-critical skills and capabilities to the project team.

2.2.2.7 A proven market leader in local and global Cyber threat detection and threat hunting tools and technologies implementation, support and maintenance. The service provider must possess technical expertise, skills and experience of minimum of 5 years on the solution.



**state security**

State Security Agency  
REPUBLIC OF SOUTH AFRICA

**NB: Only service providers who fully comply with the above requirements will be engaged in the RFP process.**

---



state security

State Security Agency  
REPUBLIC OF SOUTH AFRICA

**NON-DISCLOSURE AGREEMENT**

For as much as I .....the  
(Full name)

Undersigned (Receiving Party) with ID No: ....., am about to attend a Tender Briefing Session with regard to Tender No: SSA/23/2021-22 held by Department of State Security Agency (Disclosing Party), or have already done so, and consequently have access to classified information, I enter into an agreement with Department of State Security Agency, an entity organised and existing under the laws of the Companies Act of South Africa, with its' head office located at: MUSANDA COMPLEX, JOE NHLANHLA DRIVE, OFF DELMAS ROAD, RIETVLEI, PRETORIA EAST, RSA.

The Disclosing Party and Receiving Party agree to the following:

**1. NON-DISCLOSURE OF CONFIDENTIAL INFORMATION**

Both Parties understand and agree that each Party may have access to the confidential information of the other party. For the purposes of this Agreement, "Confidential Information" means proprietary and confidential information about the Disclosing Party's (or it's suppliers') business or activities. Such information includes all business, financial, technical, and other information marked or designated by such Party as "confidential" or "proprietary." Confidential Information also includes information which, by the nature of the circumstances surrounding the disclosure, ought in good faith to be treated as confidential. The Recipient shall use the Confidential Information only for the Disclosing Purpose and ensure proper and secure storage of all Confidential or Disclosed Information.

For the purposes of this Agreement, Confidential Information does not include:

- A. Information that is currently in the public domain or that enters the public domain after the signing of this Agreement.
- B. Information a Party lawfully receives from a third Party without restriction on disclosure and without breach of a non-disclosure obligation.
- C. Information that the Receiving Party knew prior to receiving any Confidential Information from the Disclosing Party.
- D. Information that the Receiving Party independently develops without reliance on any Confidential Information from the Disclosing Party.

Each Party agrees that it will not disclose to any third Party or use any Confidential Information disclosed to it by the other Party except when expressly permitted in writing by the other Party.

Each Party also agrees that it will take all reasonable measures to maintain the confidentiality of all Confidential Information of the other Party in its possession or control.

The Receiving Party shall take all necessary steps and precautions to protect the Confidential Information against any unauthorised access. The Receiving Party shall limit the use of and access to the Disclosing Party's Confidential Information to the Receiving Party's employees, subcontractors and agents involved in discussions relating to the Tender and shall cause such employees to comply with the obligations set forth herein.



# state security

State Security Agency  
REPUBLIC OF SOUTH AFRICA

## 2. TERM

This Agreement shall commence the day it is executed by both Parties and Parties agree to hold in confidence, Confidential Information that was disclosed during discussions and shall remain in effect indefinitely.

## 3. RELATIONSHIPS

Nothing contained in this Agreement shall be deemed to constitute either party a partner, joint venture or employee of the other party for any purpose.

## 4. SEVERABILITY

If a court finds any provision of this Agreement invalid or unenforceable, the remainder of this Agreement shall be interpreted so as best to effect the intent of the parties.

## 5. INTEGRATION

This Agreement expresses the complete understanding of the parties with respect to the subject matter and supersedes all prior proposals, agreements, representations and understandings. This Agreement may not be amended except in a writing signed by both parties.

## 6. WAIVER

The failure to exercise any right provided in this Agreement shall not be a waiver of prior or subsequent rights.

This Agreement and each party's obligations shall be binding on the representatives, assigns and successors of such party. Each party has signed this Agreement through its authorized representative.

*Thus agreed and signed on this .....day of.....2021.*

*Signature: .....*

*Name of Company: .....*

*Witness: .....*

*.....  
Signature of the Authorised Member of State Security Agency)*

*Witness: .....*