# Tender announcement

Sukarrieta, 6 March 2023

## 1. OBJECT

The AZTI Foundation announces the opening of a public tendering procedure for **the continuous monitoring of traffic against cyber-attacks (SIEM) of the networks of the 3 AZTI centres**.

## 2. LENGTH OF SERVICE

The implementation of the service shall be managed within a **maximum of 4 weeks** from the date of signature of the contract.

The contract shall have a duration of **twelve months (1 year)** from the date of signature of the contract.

## 3. ECONOMIC TENDER

The maximum economic offer that will be accepted for this tender is **seven hundred and fifty euros (€750.00) per month**, taxes not included.

Invoicing will be done on a monthly basis, and invoices will be paid within 60 days from the date of issue.

## 4. ASSESSMENT CRITERIA FOR PROPOSALS

The proposals received will be assessed on the basis of the following criteria:

| | |
|---|---|
| Economic offer | 60% |
| Technical adjustment | 25% |
| Improvements | 10% |
| CSR policies | 5% |

## 5. PRESENTATION OF THE PROPOSALS

Bidders may submit their proposals to the attention of Irati Velez at the e-mail address ivelez@azti.es and at any of the AZTI centres, from the time of publication of this announcement on the AZTI Foundation website, **until 12 noon on 21 March 2023**.

Proposals can be submitted in Spanish, English or Basque.

Tenderers may contact the following address for further **technical information**:

AZTI

César Idokiliz

Tel. 34 656 78 49 78

Mail:  cidokiliz@azti.es

## 6. AWARD

Once the offers have been received on the date indicated for their presentation, within 15 working days, the result of the tender will be published on the AZTI Foundation website.

## 7. CONDITIONS DE RECRUTEMENT

- The selected entity, during the time that the service relationship with AZTI lasts, must comply with the regulations in force on labour matters, Social Security and Health and Safety at Work, being subject, if applicable, to carry out the coordination of business activities in accordance with RD 171/2004 according to the procedure and specifications established (available at https://www.azti.es/en/recruitment-rules/)

- In any case, and independently of any other documentation, the selected entity must present, before the formalization of the contract, a certificate that proves that it is up to date with the fulfillment of its tax and social security obligations.

- The selected entity must present the necessary documentation to formalize the contract within a period not exceeding 20 days from the award. Or the documentation, the selected entity must follow the Internal Contracting Regulations published at  www.azti.es

- In addition to the technical and administrative conditions, AZTI will positively evaluate those suppliers who demonstrate that they maintain policies on Quality, Health and Safety, the Environment, Sustainable Mobility, as well as Corporate Social Responsibility.

  The supplier shall include in its proposal those documents or records that allow verification of these policies (quality and environmental certificates, documentation relating to actions in matters of social responsibility, etc.)

## 8. GENERAL DATA PROTECTION REGULATION

Person in charge: Identity: FUNDACION AZTI - AZTI FUNDAZIOA - CIF: G48939508 Postal address: TXATXARRAMENDI UGARTEA Z/G SUKARRIETA (BIZKAIA) Telephone:

946574000 e-mail: lopd@azti.es.

"From FUNDACIÓN AZTI we treat the information you provide us with the purpose of placing your order and billing for services and maintaining commercial relations. The legal basis for the processing of your personal data is our legitimate interest in maintaining commercial relations and carrying out the provision of services, being strictly necessary for this purpose. The data provided will be kept as long as the commercial relationship is maintained or for the years necessary to comply with legal obligations and, once the relationship has been resolved, to the extent that liabilities may arise. The data will not be transferred to third parties except in cases where there is a legal obligation, as well as to those providers of technical and computer services and auditing. Under no circumstances will we carry out international transfers of your personal data. You have the right to obtain confirmation as to whether or not FUNDACION AZTI - AZTI FUNDAZIOA is processing your personal data. Therefore, you have the right to access your personal data, rectify inaccurate data or request its deletion when the data is no longer necessary, as well as to exercise your right to oppose, limit or transfer your data, under the terms provided for in the applicable data protection regulations, by writing to the above-mentioned address. You may also lodge a complaint with the competent supervisory authority".

## 9. TECHNICAL REQUIREMENTS

With this contract, we are seeking the continuous monitoring of traffic against cyber-attacks (SIEM) of the networks of AZTI's 3 centres.

The system will consist of the implementation of a probe in each centre. The probes will not receive any attack if the organisation has not been compromised. Therefore, any detection made by this set of probes will launch an automatic alert that will cause the contracted company to contact AZTI immediately. Initially, a manual profiling will be carried out to analyse the usual connections within the network.

From the implementation of probes, it is possible to obtain a series of data for the profiling of the network and thus be able to create automated alarms based on behaviour that deviates from normal network use:

Thanks to all this data obtained, it is possible to create indicators of compromise for the creation of rules:

Generic:

- New MAC address
- New IP address
- ARP spoofing
- Port scanning

Contextualised based on communications history:

- Port not used so far.
- A DNS query is made to a new domain name.
- Variations in traffic volume/no. of connections with respect to history by:
  - Source/destination host
  - Source/destination port
  - Communication flow

o Time slot

Based on vulnerability analysis:

- Payloads of known malware for inventoried services
- Whitelist of protocols and ports
- Blacklist of payloads per protocol

Protocol specific:

- Read-only mode
- Communications reset.
- Clearing of counters and diagnostic registers
- Read device identifier.
- Incorrect packet length
- Communication on port other than TCP/502
- Exception code delay
- Function code scans

Every month, there will be a meeting with AZTI, where a report with these findings will be presented.