Acquisition Directorate
RFQ-CO-115300-CSSR@.ncia.nato.int

NCIA/ACQ/2020/12831
08 December 2020

Market Survey Request For Information

Network Behavioral Anomaly Detection (NBAD)

MS-CO-115300-CSSR

The NCI Agency requests information regarding potential products and solutions to enable the NATO Cyber Security Centre (NCSC) Security Operations Centre (SOC) achieve visibility of anomalous and/or malicious behavior through the analysis of network traffic captured/intercepted across the NATO estate.

NCI Agency Point of Contact
Contracting Officer, Frank Iyakaremye
RFQ-CO-115300-CSSR@ncia.nato.int

To: See Distribution List

Subject: NCI Agency Market Survey Request MS-CO-115300-CSSR
Network Behavioural Anomaly Detection (NBAD)

Reference
A. Notification of Intent to Requests for Quotations, RFQ-CO-115300-CSSR, NCIA/ACQ/2020/7085, issued 16 November 2020

1. NCI Agency requests the assistance of the Nations to identify industry contacts for an NBAD solution at the NATO Computer Incident Response Centre (NCIRC), Mons.

2. The NCI Agency reference for this MS is **MS-CO-115300-CSSR**, and all correspondence and submissions concerning this matter **must** reference this number within the documentation and email subject line.

3. This request is in reference to **Annex "A", article 2.1.2** of the **Notification of Intent to Request for Quotations Cyber Security System Refresh (CSSR)**, published on November 16th, 2020.

4. This Market Survey (MS) is being issued to obtain information on existing systems and how each solution can possibly meet our requirements as well as to identify potential NATO-nation based solutions and possible suppliers.

5. The MS scenarios are provided in Annex A. Each nation is requested to forward this MS to all potential vendors with capabilities in the area of Network behavioral anomaly detection.

6. Responses shall be submitted to the NCI Agency POC at point 9 of this letter. Respondents are invited to carefully review the questions within Annex A of this letter to determine interest.

7. Responses shall in all cases include the name of the firm, telephone number, e-mail address, designated Point of Contact, and NATO UNCLASSIFIED responses to the scenarios in Annex A. This shall include any restrictions (e.g. export controls) for direct procurement by NCI Agency.

8. The closing date for this MS is **close of business Monday, January 18, 2021**

9. Please send all responses via email to the following NCI Agency contact:

Mr. Frank Iyakaremye, Contracting Officer
E-mail: RFQ-CO-115300-CSSR@ncia.nato.int

10. Product demonstrations or face-to-face briefings/meetings with industry are not foreseen during this initial stage. Respondents are requested to await further instructions after their submissions and are requested not to contact any NCI Agency staff directly other than the POC identified in Paragraph 9 above.

11. Any response to this request shall be provided on a voluntary basis. Negative responses shall not prejudice or cause the exclusion of companies from any future procurement that may arise from this MS. Responses to this request, and any information provided within the context of this survey, including but not limited to capabilities, functionalities and requirements will be considered as indicative and informational only and will not be construed as binding on NATO for any future acquisition.

12. The NCI Agency is not liable for any expenses incurred by firms in conjunction with their responses to this MS and this survey shall not be regarded as a commitment of any kind concerning future procurement of the items described.

For the Director of Acquisition:

Ijeoma Ike-Meertens
Principal Contracting Officer (Acting)

Attachment(s):
Annex A- NBAD Market Survey Scenarios

Distribution List

- **NATO Delegations (Attn: Infrastructure Adviser)**

Albania
Belgium
Bulgaria
Canada
Croatia
Czech Republic
Denmark
Estonia
France
Germany
Greece
Hungary
Iceland
Italy
Latvia
Lithuania
Luxembourg
Montenegro
The Netherlands
North Macedonia
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Turkey
United Kingdom
United States

- **NATO HQ**

NATO Office of Resources, Management and Implementation Branch – Attn: Deputy Branch Chief
Director, NATO HQ C3 Staff, Attn: Executive Coordinator
SACTREPEUR, Attn: Infrastructure Assistant
SHAPE, Attn: J3 & J2

- **Strategic Commands**

HQ SACT Attn: R&D Contracting Office
ACO Liaison Office

- **All NATEXs**
- **NCI Agency – Internal**

Annex A- Network Behavioral Anomaly Detection (NBAD) Request For Information

1. Purpose

1.1. The NCI Agency requests information regarding potential products and solutions to enable the NATO Cyber Security Centre (NCSC) Security Operations Centre (SOC) achieve visibility of anomalous and/or malicious behavior through the analysis of network traffic captured/intercepted across the NATO estate. The NCI Agency is interested in solutions (comprised of one or more products integrated) that can enable the use case as defined in the next section.

1.2. Issuance of a Market Survey (MS) is viewed as the fastest, most efficient approach in which fairness can be upheld.

1.3. For Section 3 below, responders are requested to describe how their solution would address the use case highlighted. Responders are also welcome to further articulate how their solution would be utilized for broader cybersecurity network behavior analysis applications in a trans-national, heterogeneous military network environment.

1.4. Responses to Section 3 are not to exceed one (1) page for each scenario and in no less than Arial 12 font size. Respondents should include standard brochures as a supplement to demonstrate the capabilities of an interested party.

1.5. In Section 4, a Rough Order of Magnitude in a native MS Excel is requested.

2. Important Notes

2.1. The MS is solely a request for information, to support requirements and approvals. It shall not be treated as a request for quotation or an invitation for bids. The Agency will consider and analyse all information received from this MS and may use these findings to develop a future Request for Quote (RFQ) for a Network Behavioral Anomaly Detection system.

2.2. Any future RFQ would be advertised on the Agency's bulletin board for all eligible companies to respond. Participating in this MS will not benefit, or prejudice, involvement in any future RFQ. Any future procurement is likely to request the provision, delivery, installation and configuration of NBAD-related hardware, software and associated support.

3. Market Survey Scenarios

3.1. Monitors, alerts, and reports upon behavioural anomalies in network traffic – primarily typical corporate network IPv4 and IPv6 traffic (including Internet of Things and cloud services), but also potentially other networking protocols including industrial control systems.

3.2. Profiles behaviours across variable temporal ranges, fixed baselines, or configurable logical representations of user and system activities, in both alerting and observation-only modes.

3.3. Filters and tunes the solution to target or exclude networks, subnets, groups of systems or users, applications, protocols, or other administratively defined logical groupings including lists to block, allow, or ignore discrete selections.

3.4. Derives meaningful, contextual information regarding encrypted (for example, Transport Layer Security) or proprietary protocol network sessions.

3.5. Utilises machine learning (ML) or artificial intelligence (AI) based approaches to performing the processing and analysis of network traffic to increase the value and signal-to-noise ratio of alerts being generated by the solution.

3.6. Provides intuitive and cohesive visualisation and search capabilities, including isolation of individual sessions of traffic and the context surrounding them.

3.7. Integrates with NATO's enterprise Splunk solution to enable a single point of reference for security analysts and other stakeholders.

4. Rough Order of Magnitude (ROM) price data

4.1. Please provide a ROM pricing data for solution. The ROM submission shall in an MS Excel and in a native format.