Market Survey – Request for Information

External Attack Surface Monitoring Tool (EASM)
NCI Agency Reference: MS-115917-EASM

NCI Agency to seek industry responses regarding the availability of External Attack Surface Monitoring (EASM) solutions from within NATO nations.

NCI Agency Point of Contact
Frank Iyakaremye, Contracting Officer
Frank.Iyakaremye@ncia.nato.int

To: Distribution List (Annex A)

Subject: **NCI Agency Market Survey**
                Request for Information MS-115917-EASM

1. The NCI Agency to seek industry responses to the Agency's questions regarding the availability of External Attack Surface Monitoring (EASM) solutions from within NATO nations.

2. The NCI Agency requests the broadest possible dissemination by the Nations of this Market Survey Request to their qualified and interested industrial base.

3. The NCI Agency reference for this Market Survey Request is **MS-115917-EASM**, and all correspondence and submissions concerning this matter should reference this number.

4. Respondents are requested to reply via the questionnaire at Annex B.

5. Responses may be issued to the NCI Agency directly from Nations or from their Industry (to the Point of Contact indicated at Paragraph 9 below).

NATO Communications
and Information Agency

Agence OTAN d'information
et de communication

Avenue du Bourget 140
1140 Brussels, Belgium

www.ncia.nato.int

6. Responses shall in all cases include the name of the firm, telephone number, e-mail address, designated Point of Contact, and a <u>NATO UNCLASSIFIED</u> response to our questions in Annex B.

7. Interested parties are responsible for adequately marking proprietary or competition sensitive information contained in their response.

8. Responses are requested to be submitted by no later than **05 July 2023**.

9. Please send all responses via email to:

Frank Iyakaremye

NCI Agency, Acquisition

Frank.Iyakaremye@ncia.nato.int

10. The RFI 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 RFI and may use these findings to develop a future RFQ for External Attack Surface Monitoring (EASM) solutions. Any future solicitation would be advertised on the Agency's bulletin board for all eligible companies to respond. Participating in this RFI will not benefit, or prejudice, involvement in any future solicitation.

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 Market Survey. Responses to this request, and any information provided within the context of this survey, including but not limited to pricing, quantities, capabilities, functionalities and requirements will be considered as information 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 Market Survey and this Survey shall not be regarded as a commitment of any kind concerning future procurement of the items described.

13. Your assistance in this Market Survey request is greatly appreciated.

For the Director of Acquisition:

//signed//

Frank Iyakaremye
Contracting Officer

<u>Enclosures</u>:
Annex A, Distribution List
Annex B, Summary of Requirements & Questionnaire

ANNEX A
Distribution List for Market Survey

NATO Delegations (Attn: Investment Adviser)

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

Belgian Ministry of Economic Affairs

Embassies in Brussels (Attn: Commercial
Attaché) Albania
Belgium
Bulgaria
Canada
Croatia
Czech Republic

Denmark
Estonia
France
Germany
Greece
Hungary
Iceland
Italy Latvia
Lithuania
Luxembourg
Montenegro
Netherlands
North
Macedonia
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Türkiye
United Kingdom
United States of America

ANNEX B

External Attack Surface Monitoring Tool (EASM) Request For Information

Purpose

The purpose of this RFI is to seek industry responses to the Agency's questions regarding the availability of External Attack Surface Monitoring (EASM) solutions from within NATO nations.

In this context, the External Attack Surface Monitoring (EASM) is a solution that enables organisations to continuously monitoring the attack surface through ongoing discovery, inventory and security analysis of the digital assets exposed to external attacks.

Issuance of an RFI is viewed as the fastest, most efficient, approach in which fairness can be upheld. The Agency is looking for a NATO nation provided solution that is comprised of one or more integrated products enabling cybersecurity teams to determine and fine-tune our cyber security posture of the externally-facing assets.

Each question will request advice from industry about a specific issue, and responses are expected to solicit information from vendors about their current solutions. Responses are not to exceed one (1) page for each question in no less than 12 font size. Vendors should include standard brochures as a supplement to demonstrate the capabilities of an interested party.

Important Notes

The RFI 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 RFI and may use these findings to develop a future RFQ for External Attack Surface Monitoring (EASM) solutions. Any future RFQ would be advertised on the Agency's bulletin board for all eligible companies to respond. Participating in this RFI will not benefit, or prejudice, involvement in any future RFQ.

RFI Questions

1.   NCIA is seeking a solution based on NATO nation products and/or services. Please indicate the name and national origin of the parent company for each product or service you are including in your survey response.

2.   Please detail how if the customer's data is protected and in which geographical location it is stored.

3.   Can your solution provide the following capabilities (please mark each applicable item):

☐   Internet exposed assets detection and inventory
☐   External Attack surface visibility
☐   Exposure detection and prioritization

Please describe how your solution achieves these capabilities.

4.   Please describe how your solution provides user/access management. Is the process for adding users only done from a higher solution level (authorized by the solution administrators) or can users be added locally (authorized by the customer administrator)?

5.   Has your solution the capability of grouping assets and provide tailored access based on group membership.

6.   Please describe how the scans are executed on the discovery assets with your solution. What is the scan frequency? Is it possible to launch a manual scan at specific time? Is the execution of manual scan correlated with the cost model?

7.   Please describe how the tool is prioritizing assets for analysis and risk assessments, does it provide a risk score, or a ranking system, for assets based on their importance and vulnerability?

8.   Please describe how the solution can provide accurate detection results, with clear details on what actions are executed to reduce potential false positive.

9.   Please describe how to define a scope for assets discovery (for example by DNS seeds, IP ranges, etc). How is the tool able to identify changes to existing assets?

10.   Please describe how your solution can be integrated with third-party tools and external repositories.

11.   Please describe if your solution is capable of adding custom-made checks on demand of the customer.
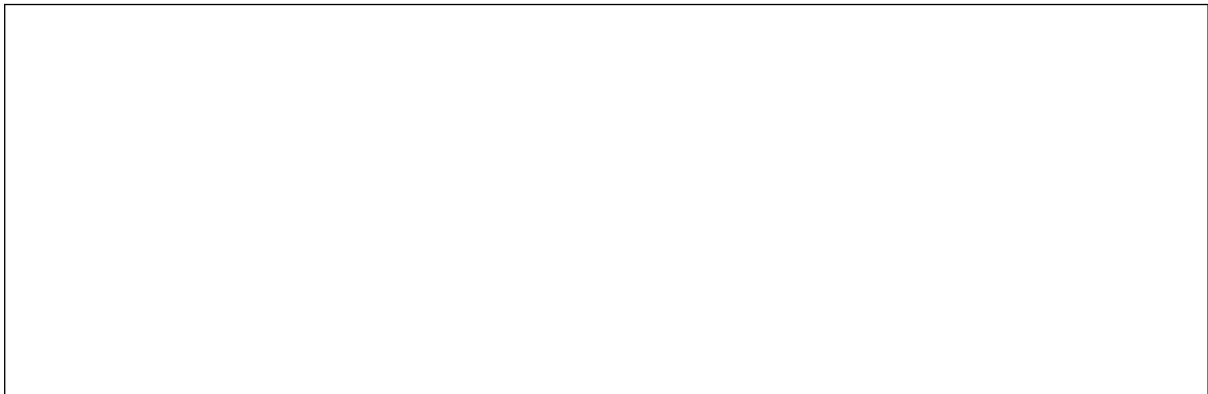
12.   Please describe how your solution provides the ability to show historical information of detected assets and associated issues. What is the data retention policy?

13.   Does your solution provide the ability to view details such as source code of any conducted test? Please describe.

14. Please illustrate how your solution supports alerting mechanism when a specific event occurs. Can these events be customized?

15. Please illustrate how your solution provides the ability to create highly customized dashboards within the platform, to meet reporting requirements.

16. Please illustrate how your solution performs active and passive scans.