NATO Communications and Information Agency

Acquisition Directorate
NCIA/ACQ/2023/07292
19 September 2023

Market Survey – Request for Information

Cyber Threat Intelligence

NCI Agency Reference: MS-422211-CTI

NCI Agency is seeking information from Nations and their Industry in order to assess availability of Commercial-Off-The-Shelf (COTS) Cyber Threat Intelligence products.

NCI Agency Point of Contact
Sumiko Duncan, Senior Contracting Officer (Consultant)
Sumiko.Duncan@ncia.nato.int

To: Distribution List (Annex A)

Subject: **NCI Agency Market Survey**
Request for Information MS-422211-CTI

1. The NCI Agency requests the assistance of the Nations and their Industry to identify available Commercial-Off-The-Shelf (COTS) Cyber Threat Intelligence products.
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-422211-CTI**, 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 NATO UNCLASSIFIED description of the capability available and its functionalities. This shall include any restrictions (e.g. export controls) for direct procurement of the various capabilities by the NCI Agency. Non-binding product pricing information is also requested as part of the questionnaire.

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 **Monday, 16 October 2023**.

9. Please send all responses via email to:

Sumiko Duncan

NCI Agency, Acquisition

sumiko.duncan@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 solicitation for Cyber Threat Intelligence products. 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//

Sumiko Duncan
Senior Contracting Officer (Consultant)

Enclosures:
Annex A, Distribution List
Annex B, Summary of Requirements & Questionnaire

ANNEX B

Summary of Requirements

The Cyber Threat Intelligence (CTI) solution enables organisations to create and gather threat intelligence, providing understanding of the threat actor's motives, targets and attack behaviors and provides data-driven actions to minimize the risk of cyber-attacks.

The Agency is looking for a NATO nation based solution that provides the capability to enable cybersecurity teams to create threat intelligence by collecting raw threat information from multiple sources (internally created feeds or industry-leading threat intelligence feeds), correlating and analyzing the data and allowing dissemination of threat information to customizable target groups and NATO's SIEM solution.

RFI Instructions

- You may either enter your responses under the questions on the following pages, or use a separate document to provide your responses.
- Please feel free to make assumptions, however, it is important that you state what these assumptions are.
- Please do not enter any general company marketing or sales material as part of your specific responses within this market survey. Please submit such material as enclosures with the appropriate references within your replies.
- Please do try and answer the relevant questions as comprehensively as possible, providing as much detail as necessary.
- Responses are not to exceed one (1) page for each question in no less than 12 font size.
- Cost details requested in the questions refer to Rough Order of Magnitude (ROM) Procurement, not a binding offer. Please include all assumptions the estimate is based upon:
    - Advantages & disadvantages of your product/solution/organisation,
    - Any other supporting information you may deem necessary including any assumptions relied upon.
- Other supporting information and documentation (technical data sheets, marketing brochures, catalogue price lists, descriptions of existing installations, manuals, etc.) are also desired.

RFI Questions (1- 15)

1. Please provide your:
    a. Company name and address
    b. Point of Contact name, title and email address
2. 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.

    Please detail all export controls on any solutions mentioned in your answers to questions 3-12 below.

COTS Solution

3. Please refer to the Table at B-1 and indicate the requirements that your proposed system/technology provides (fully or partially). For each of these, provide details how the requirement is fulfilled. Add as many lines as needed.
4. Is your proposed system/technology currently in active service as a COTS solution? If so, where and what types of support (software updates, spares, onsite support, training) does your organisation currently provide for such a capability?
5. Please provide the following information regarding current and previous uses of your available COTS solution:
    a. Names of customers/users and contact details of their POC's.
    b. UNCLASSIFIED details on the specific program your COTS solution supported.
    c. Overview of any modifications to the COTS solution necessary to support these customers and the licensing terms applicable to modifications of the COTS product, stating also whether those will be assigned to the NCI Agency (Foreground/Background IPR).
    d. Estimated cost to the purchaser for modifications.
    e. Estimated size of analyst team using the solution.
    f. Estimated size of IT administrator team managing the solution.
6. Please provide us with any additional capabilities of your COTS solution that go above and beyond those already mentioned in this RFI.
7. Advantages & disadvantages of your product/solution/organisation,
8. Any other supporting information you may deem necessary including any assumptions relied upon.

Previous NATO or Equivalent National Defence Experience

9. Is your solution eligible for Security Certification through NATO or equivalent NATO nations defence process?
10. Has your solution achieved Security Certification and/or Accreditation through the NATO or equivalent national defence process? Please list any other of your solutions where such certification was achieved.
11. Has your solution achieved approval through the NATO Request for Change (RFC) or an equivalent national defence process? Please list applicable past projects.

Pricing, Support, Miscellaneous

12. Please provide Rough Order of Magnitude pricing information for your solution so that the Agency has a general idea of the pricing model and potential cost. Please include estimated costs for your current COTS solution and/or the criteria to calculate that cost.
    a. Are estimated fees recurring or non-recurring, and are these estimated inclusive of maintenance and support costs?
13. Does your company provide additional support services? If so, please describe what is available and the pricing.
14. Does your company offer enterprise professional support? If so, please describe what is available and the pricing.
15. Please feel free to add any information you may think that may be of value to NCI Agency. Should you need additional space, please copy this page and continue with the appropriate page numbers.

Table B-1

1	**Threat Data Collection**	Details (input from vendor)
1.1	Provides enrichment of real-time threat intelligence from industry-leading threat intelligence feeds and information-sharing communities (e.g., Malware Information Sharing Platform - MISP). (Please specify the feeds and protocols/formats supported)	
1.2	Allows ingestion of custom feeds, supporting files in various templates and formats (e.g. internal security data from SIEM, EDR, XDR; vulnerability data including customer-specific vulnerabilities in standard/open formats, etc.). (Please specify the systems, templates and formats supported)	
2	**Feeds processing**	
2.1	Provides automated processing (aggregation, normalization) of collected feeds.	
2.2	Provides automated processing (correlation) of collected feeds and identifies trends and patterns in the data.	
2.3	Allows tracking and mapping of adversary tactics and techniques with frameworks such as MITRE ATT&CK.	
3	**Intelligence analysis**	
3.1	Allows analysts to annotate intelligence data with customer-and context-specific information.	
3.2	Allows for analysts to perform queries.	
3.3	Provides anomaly-based analysis.	
3.4	Provides workflow automation for threat investigations.	
3.5	Allows analysts to create profiles of adversaries (manually).	
3.6	Capable of generating alerts automatically based on collected intelligence.	
3.7	Allows analysts to generate alerts manually based on collected intelligence and analysis results.	
3.8	Allows prioritization of analyst work (i.e. based on intelligence alerts or other means).	
3.9	Allows analysts to collaborate on tasks and share datasets.	
3.10	Provides analysts with a research sandbox which supports isolation and dynamic analysis of files in various templates and formats.	
3.11	Allows analysts to perform other intelligence analysis activities. (Please describe)	
4	**Intelligence dissemination**	
4.1	Allows manually disseminated report feeds, technical feeds or custom threat intelligence feeds.	

4.2	Allows automatically disseminated report feeds, technical feeds or custom threat intelligence feeds.	
4.3	Allows automated information-sharing with MISP.	
4.4	Allows data to be shared with security tools such as SOARs, XDRs and SIEM.	
4.5	Allows alerts to be automatically generated in security tools (e.g. for active attacks).	
4.6	Allows risk scores for threat prioritization to be assigned in security tools.	
4.7	Allows other actions to be triggered in security tools. For example, is it possible to dynamically adjust monitoring/logging parameters based on the collected threat intelligence? (Please specify the tools and actions/APIs/standards supported)	
4.8	Wide range of export formats: Export IOCs (Indicators of Compromise) or actionable context into widely used, more organized machine-readable sharing formats, such as STIX, OpenIOC, JSON, Yara, Snort or even CSV.	
4.9	Allows control and management of information sharing.	
4.10	Allows integration with threat hunting processes.	
5	**Solution requirements**	
5.1	Supports high availability (redundancy).	
5.2	Allows incoming feeds to be monitored.	
5.3	Allows system health to be monitored.	
5.4	If hosted service, specify where the data is hosted.	
5.5	Follows one or more industry-standard deployment models (e.g. dedicated appliance, on premise virtual machine, on premise container, cloud service, hybrid). If hybrid, please indicate the solution components offered through each deployment model.	
5.6	Runs on one or more major operating systems (e.g. Windows, Linux).	
5.7	If applicable, any runtime components run on one or more major runtimes (e.g. .NET, JRE, Docker).	
5.8	If applicable, any database components run on one or more major databases (e.g. MS SQL, Oracle, postgreSQL, MongoDB).	
5.9	Support transferring threat intelligence through multiple information classification levels with data diodes (i.e. through file, TCP, and/or UDP transfers).	
6	**Management**	
6.1	Uses a documented API for integration with 3rd party systems.	
6.2	Allows automated configuration checks using documented API	

6.3	Allows complete/partial configuration import and export	
6.4	Manages policies, deployment, compliance, and reporting from a single, centralized console	
6.5	Allows export of management policies in human and machine readable format (e.g. XML)	
6.6	Has log capabilities for all its components, where logs can be collected centrally by the customer (e.g. Splunk, ArcSight).	
6.7	Has configurable reporting capabilities, including multiple report formats (e.g. PDF, XML) and distribution methods (e.g. email, web portal, RSS)	
6.8	Allows a customer to configure alerting policy/rules for collected intelligence based on the customer's requirements.	
6.9	Has configurable alert formats (e.g. Syslog, Windows Event, email, SNMP).	
6.10	Allows manual and automated updates of software components.	
6.11	Allows online and offline, configurable software update sources	
6.12	Works both in environments connected to Internet and in environments without Internet connectivity. Please indicate any functionality available only through Internet connectivity.	
6.13	Graphical user interface to the management console is browser based, using HTML 5 technology (not using Flash/Activex/Java components on the client side)	
6.14	Uses role based access control (RBAC), providing granular read/write user roles.	
6.15	Allows both local definition of users and roles and integration with central identity and access management solutions (e.g. AD).	
6.16	Solution is able to undergo penetration testing and vulnerability assessment by the customer. Please indicate any specific requirements for security assessments of the solution.	
7	**Support**	
7.1	Provides Train-the-Trainer courses for NCIA personnel (a total maximum of 20 pupils to allow future in-house training of all roles without external contractor support).	
7.2	Offers multiple support channels (phone/email/web portal/chat).	
7.3	Uses qualified, dedicated support staff.	
7.4	Applies specified response and resolution timeframes.	