NATO Communications and Information Agency

Acquisition
NCIA/ACQ/2023/07582
21 December 2023

Request for Information

Cyberspace Deception Technologies
NCI Agency Reference: MS-423222-CDT

NCI Agency seeks to identify the availability and technical capability of qualified NATO Industry sources for commercial products to provide the required cyberspace deception COTS solutions.

NCI Agency Point of Contact
Ms. Sumiko Duncan, Senior Contracting Officer (Consultant)
MS-423222-CDT@ncia.nato.int

To: Distribution List (Annex A)

Subject: **NCI Agency Market Survey**
Request for Information MS-423222-CDT

1. Through issuance of this notice, the NCI Agency seeks to identify the availability and technical capability of all qualified NATO nation businesses that believe they can provide the services described in this announcement.
2. This is a Request for Information (RFI). It is NOT a solicitation for proposals nor a pre-solicitation notice.
3. The NCI Agency reference for this RFI is **MS-423222-CDT**, and all correspondence and submissions concerning this matter should reference this number.
4. The NCI Agency requests the broadest possible dissemination by the Nations of this RFI to their qualified and interested industrial base.

5. The information resulting from this effort is for planning purposes only and for assisting the NCI Agency in refining its requirement and related acquisition strategy. As a result, the NCI Agency will not pay for any costs incurred in responding to this RFI.
6. Responses may be issued to the NCI Agency directly by eligible NATO industry to the Point of Contact indicated at Paragraph 10 below.
7. Responses shall follow the instructions for submittal at Annex B of this RFI.
8. Interested parties are responsible for adequately marking proprietary or competition sensitive information contained in their response.
9. Product demonstrations or face-to-face briefings/meetings with industry are not foreseen during this initial stage, however technical discussions may take place following the submission of responses, with the purpose of clarifying or further augmenting those responses where required
10. Responses are requested to be submitted to Ms. Sumiko Duncan via email at MS-423222-CDT@ncia.nato.int by 15 February 2024.
11. Your assistance in this RFI is greatly appreciated.

For the Chief of Acquisition:

Sumiko Duncan
Digitally signed by Sumiko Duncan
Date: 2023.12.21 15:39:12 +01'00'

Sumiko Duncan
Senior Contracting Officer (Consultant)

Enclosures:
Annex A, Distribution List
Annex B, Instructions & Questionnaire

Distribution List

NATO Delegations (Attn: Military Budget Adviser)

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

MS-423222-CDT Instructions & Questionnaire

Background

1. Cyberspace deception technologies are a category of cybersecurity solutions which can be defined as deliberate deployment of fake digital assets to lure adversaries in order to obtain real-time targeted actionable intelligence, providing early warning of potential cyber security attacks, alerting organizations of unauthorized activity, and understanding whether the currently deployed security controls are effective. Deception technologies products can detect, analyse, and defend against zero-day and advanced attacks. Deception can also provide, among other things, critical risk management information, Adversary-Generated Threat Intelligence (AGTI), Adversary Deflection and Adversary Management, protection of critical assets and Cyberspace Situational Awareness. Deception can protect operational assets throughout the Enterprise, in the field, or while engaging with Cyber Threat Actors (CTAs).
2. This Markey Survey seeks insight on commercial products to provide cyberspace deception COTS solutions and to assess the ability to use a deception solution for alternative/ supporting roles such as cyber range, training, etc.

3. NCI Agency is interested in learning more about the following types of solutions: External Cloud-based solution; On premises solution (assumed in Belgium); and a Hybrid solution.

Instructions for Submitting a Response:

1. Interested and eligible organizations from a NATO nation possessing the capabilities to meet the needs described herein, along with the experience in having supported similar needs should submit one (1) electronic response to MS-423222-CDT@ncia.nato.int. Responses shall be submitted no later than close of business on 15 February 2024 and shall contain **no classified material**:

   a. **Part I - A cover sheet clearly identifying the following information**:

   - Re: reference control number MS- 423222-CDT;
   - Organization name, address, and contact information (telephone number and email address of designated Point of Contact);
   - A brief description of your business or organization, including the main products and services it offers and the market or customers it primarily supports. This should include information on where your solution is deployed within your (or other NATO) nation, overview of that deployment and how it may relate to this market survey, and how your organization will meet the needs of the services required by NATO.

   b. Part II-Capability Package consisting of:

   - Any initial assumptions, constraints, and exceptions regarding this RFI;
   - A Strengths, Weaknesses, Opportunities & Threats (SWOT) analysis of your solution.
   - A detailed technical response tailored specifically to NCIA's needs, addressing the questionnaire content provided at Annex B of this RFI.

2. Please do not enter any general company marketing or sales material as part of your specific responses within this RFI. Please submit such material as enclosures with the appropriate references within your replies.
3. Cost details requested in the questions are not a binding offer. Please include all

conditions related to the estimate provided.

4. Other supporting information and documentation (technical data sheets, marketing brochures, catalogue price lists are also desired).

MS- 423222-CDT RFI Questionnaire

Technical

Please describe how your solution would provide the following:

a. **Pre-Breach Detection** by means of deception techniques which can identify early stages of the cyber kill chain, reconnaissance, initial access, and delivery. The solution shall be able to redirect the adversary to a deception, simulated or controlled environment and provide relevant and actionable information (e.g. from purely technical Indicators of Compromise (IoCs) to threat intelligence on Tactics, Techniques and Procedures (TTPs)).

b. **Adversary Deflection** by means of active and passive digital breadcrumbs to attract an adversary, who has gained access to a NATO CIS, into a deception environment and away from production assets.

c. **Adversary Management** by means of but not limited to deploying active and/ or passive breadcrumbs, thwarting the adversary's efforts, or shutting down the adversary's access, and overall the deception management console shall allow operators to manage an adversary in real-time.

d. **Lateral Movement** of compromised hosts/accounts or by a malicious internal user.

e. **Digital Twins** of critical hosts, servers, systems, or network to ensure similarities with a real NATO environment.

f. **Exfiltration Detection** notifications by means of but not limited to, active or beaconing breadcrumbs. If the data is exfiltrated, opened, or moved (within the deception environment) the breadcrumb shall trigger a notification to specific deception operators.

g. **Realistic Cyber Training Environment** in support of Blue Team / Red Team exercises, to practice an operational scenario, gather information as to how the operational activities appear, and practice responses. The training environment should be a functional equivalent to the deception environment.

DECEPTION ASSETS				
		YES	NO	COMMENTS
1	Does the solution provide the ability to run in production environments, in a safe manner, and at scale?			
2	Is the solution able to create centrally managed realistic deception assets and networks on real virtual machine assets (not emulated)?			
3	Is the solution deployable both within a commercial deception host mimicking the production network and an actual production network including a high security air-gapped network?			
4	Does the solution allow for flexible deployment capability between production and deception assets (Cloud, on premises and hybrid)?			
5	Is the solution flexibly deployable on different platforms, providers and practicable types of servers? For example, Active Directory, file server, Mail server, Gitlab server, OT, Web			

	server, etc.			
6	Can the solution instrument golden image hosts (physical or virtual of any operating system)?			
7	Does the solution simulate user and administrator behavior within deception environments creating a dynamic, changing deception environment?			
8	Does the solution produce and deploy (manual and automated) deceptive digital breadcrumbs, beaconing breadcrumbs and realistic pocket litter throughout both a commercial deception host mimicking the production network and an actual production network including a high security air-gapped network?			
9	Is the solution able to deceive and confuse the adversary as to what is production versus non-production assets?			
COMMUNICATION WITH DECEPTION ASSETS				
10	Does the solution provide secured communications for intelligence and counter-intelligence collection as well as for Command and Control (C2) of all deception assets? *I.e., that all agents involved in the C2 aspects are authenticated, all information exchanges/ C2 support integrity controls to withstand Distributed Denial of Service (DDoS) or other availability attacks.*			
11	Does the solution provide automated secure connection between proxies for ease of deployment and tear-down?			
12	Does the solution supply redundancy of communications within a layered deception proxy deployment?			
13	Does the solution store threat intelligence and C2 information locally for later transmission? If yes, is the data always stored in encrypted form?			
CENTRALLY MANAGED DECEPTION				
14	Is the solution deployable and manageable from a centralized web console with the ability to create and deploy active and passive digital breadcrumbs, honey tokens and pocket litter?			
15	Can the solution design and create attack paths within a deception or hybrid environment with deceptive users, groups, services?			
16	Is the solution able to create and deploy various breadcrumbs / honey tokens / pocket litter including those for purposes of testing			

	the efficacy of the attack path design?			
17	Can the solution instrument and gather threat intelligence without detection in the environment by the adversary, including in such cases when no external communication access is available?			
18	Can it track the deployment of deceptive breadcrumbs and assets allowing a complete clean up after campaign completion?			
19	Is it able to provide real-time alerting of any access to the deception assets including beaconed breadcrumbs?			
20	Does it record and collect encrypted syslog, service logs, full user telemetry, hashes, Indicators of Compromise (IOCs), TTPs and any other threat intelligence data on every action an adversary takes within the deception environment?			
21	What does it provide the ability to replay, for training purposes? (i.e., known attacks and TTPs of major CTAs).			
22	Is the solution able to track misleading / fake information across different deception hosts / campaigns / networks?			
ADVERSARY-GENERATED THREAT INTELLIGENCE				
23	Can the solution categorize and provide context to, as well as perform automatic analysis of the gathered threat intelligence?			
24	Can it perform automatic mapping of CTA events to the MITRE ATT@CK Framework?			
25	Can it perform automatic recommendation of engagement from the MITRE ENGAGE Framework?			
26	Can it provide automated prediction of an adversary's possible next steps?			
27	Does it provide (predictive) automated and manual response, rules and engagement with an adversary based on observed behavior?			
28	Is the solution capable of integration with SIEM, SOAR, MISP and ingestion of events from deception assets?			
29	Does the solution automatically reduce the noise or false positives of collection of syslog, service logs, full user telemetry, hashes, IOCs and TTPs?			
30	Does the solution extract TTPs used by the adversary to attack mimicked infrastructure?			
31	Does the solution perform actions and collect information on a deception host in stealth mode or without the adversary noticing?			
32	Does the solution capture all the TTPs of an adversary and then replay them in the			

	deception environment for training or operations?			
33	Is the solution able to format all gathered threat intelligence in standard threat intelligence formatting to automate the sharing of threat intelligence with various platforms? (such as MRTI , STIX2 , APIs)			
34	Does the solution alert on new TTPs and tools not previously reported?			
SECURITY / NON-TECHNICAL				
35	Does the solution allow strict compartmentalization for operators belonging to different campaigns (i.e. operators associated to given campaigns shall not be able to access any data relevant to and generated by other campaigns)?			
36	Is it possible to have read only access to security auditors who shall be able to access data for all campaigns?			
37	Has the solution been developed following an approved standard Secure Software Development Lifecycle (SSDLC)?			
38	Does the solution support two factor authentication?			
39	Who owns the information generated and/ or handled by the solution during the execution on a contract, or during any 'proof of value'?			
40	Does the solution support long term storage of all campaign information? If yes, is it locally stored or offline? For how long?			
41	Are there integrity controls for campaign information collected? If yes, explain how it supports a forensics chain of custody.			

42. 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 the services you are including in your questionnaire response (list should also include subcontractors if applicable).
43. Provide information of any Facility Security Clearance (FSC) that has been granted to the company, specifying classification level and whether it includes ability to store NATO Classified Information in physical form and/or digitally.
44. Are any of the tools listed already security certified and/or accredited through NATO or equivalent national defense process? If yes, please list which ones.
45. Is the solution accredited for use within a Classified environment in a NATO nation?
46. Is the solution accredited to handle NATO Classified Information?

Pricing

47. How are your services priced? Please provide ROM pricing data for the solution broken down for the three options:
    i. Option A: External Cloud-based solution;
    ii. Option B: On premises solution (assumed in Belgium);
    iii. Option C: Hybrid solution.
48. Please provide ROM pricing data on potential additional support services including training required to operate and maintain the solution.
49. Please provide ROM pricing data on potential enterprise professional support services taking into consideration that personnel with valid NATO security clearance up to and including NATO SECRET level might be necessary for support as required.
50. Does your pricing model offer a reduced rate for extended contracts beyond one year?
51. What are your payment terms?

Other

52. Please feel free to add any information you may think that may be of value to NCI Agency.