NATO Communications and Information Agency

Acquisition

NCIA/ACQ/2024/06877

24 May 2024

Request for Information

Endpoint Protection and Response Landscape
NCI Agency Reference: RFI-423270-EDR

NCI Agency seeks to identify state-of-the-art Endpoint Detection and Response (EDR) solutions that can be provided through Commercial of the Shelf (COTS) products, solutions and/or services that will assist NCIA and its customers at a NATO Enterprise create an accurate and current view of these solutions and decide on the next steps to set up an Invitation for Bid.

NCI Agency Point of Contact

Ms. Leonora Alushani, Contracting Officer

RFI-423270-EDR@ncia.nato.int

To: Distribution List (Annex A)

Subject: **NCI Agency Market Survey**
Request for Information RFI-423270-EDR

1. Through issuance of this notice, the NCI Agency seeks to identify the availability and technical capability of all qualified NATO nation businesses that 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 **RFI-423270-EDR**, 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.

NATO Communications and Information Agency

Agence OTAN d'information et de communication

Avenue du Bourget 140
1140 Brussels, Belgium

www.ncia.nato.int

5. The information resulting from this effort is for assisting the NCI Agency in understanding the existing technologies, their maturity level, identifying potential NATO nation based solutions and possible suppliers and defining requirements that will become part of an IFB package to be released to industry in the near future.

6. Responses may be issued to the NCI Agency directly by eligible NATO industry to the Point of Contact indicated at Paragraph 11 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. Technical demonstrations may take place following the submission of responses, with the purpose of showcasing your solution and clarifying or further augmenting those responses where required. Product demonstrations and/or face-to-face briefings/meetings with industry may be considered with companies that have submitted a formal response to this RFI.

10. The NCIA will consider and analyze all information received from this RFI and will use these findings to develop a future solicitation for an EDR product, solution and/or services. Any future solicitation would be advertised on the Agency bulletin board for all eligible companies to respond.

11. Responses are requested to be submitted to Ms. Leonora Alushani via email at RFI-423270-EDR@ncia.nato.int by 17 June 2024.

12. Your assistance in this RFI is greatly appreciated.

For the Chief of Acquisition:

Leonora Alushani
Contracting Officer

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
Turkiye
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
Turkiye
United Kingdom
United States of America

RFI-423270-EDR Instructions & Questionnaire

Purpose of this Request for Information

The purpose of this Request for Information (RFI) is to create an accurate and current view of the state-of-the-art of Endpoint Detection and Response (EDR) solutions that can be provided through Commercial of the Shelf (COTS) products, solutions and/or services.
The feedback received through the RFI will be used to evolve existing endpoint protection and EDR capabilities in NATO and define future needs. The inputs will be used to help NATO define future requirements within these capabilities and to shape future acquisitions.
Responses should focus on current mature solutions, products or services, although responders are also provided an opportunity in a separate section to volunteer details of evolutionary plans and future roadmaps.
This RFI is divided in two parts:

- Categories of interest for the respondent to provide information to.
- Breakdown of the categories in detailed questions.

To the extent possible and where applicable, the respondent is requested to provide a response to the detailed breakdown. Responses may be supported by external references such as product documentation, technical data sheets and websites where applicable. In such cases, please ensure that any references are direct to relevant products, solution and/or services, rather than general references (e.g. to the company website).
Thank you for taking the time to provide your responses.

****** Please respond to the questions indicating the exact product name(s) and version(s) providing the function and also identify differences on applicability to different endpoint types (e.g. Windows vs. Linux vs. iOS) and differences between implementation types (e.g. cloud connected vs. air-gapped).***
Please note that individual responses will not be shared with others responders or third parties.

RFI RESPONSE CATEGORIES

1. **Company overview:** Company details and track record in providing solutions and services in for the cyber security industry. Particular interest goes out to EDR solutions and your experience providing them to Defense industries and international organizations such as the EU and NATO.

2. **Solution overview and deployment model:** Overview of EDR products suite, providing details related to the architectural design, central management, the use and deployment of agents, scalability and cloud integration.

3. **Product features and capabilities:** Functions and capabilities provided by the EDR products suite, detailing unique features, coverage, and performance indicators.

4. **Data collection, processing and storage:** Types of data that can be collected, processing methods, and details related to how data is stored and secured.

5. **Threat intelligence and threat hunting:** Overview of threat intelligence integration capabilities; of particular interest are (1) feeds provided through your team and solution, and (2) integration of external feeds through industry exchange standards.

6. **Policy management:** Overview of policy and playbook management. Specific interest goes out to privilege management, central vs. per site policy application, customization of policies and playbooks, and version control.

7. **System integration:** Integration capabilities of the EDR suite with other (security) systems. Please detail both integration with own products and features as well as those provided by other vendors.

8. **Tool security:** Security functions and measures taken to guarantee the security of the system and its data.

9. **Management:** The means and mechanisms included to manage the EDR product suite, with a specific interest for large distributed implementations with a large number of stakeholders.

10. **Support, maintenance and service provisioning:** Services provided to ensure an optimal and up-to-date solution.

11. **Cost and licensing:** Breakdown of pricing and licensing of the EDR product suite, including on-demand scaling requirements.

12. **Roadmap and future development:** Planned products and features in the near-future with associated timelines.

13. **Case studies and success stories:** Overview of recent references and success stories to highlight experience. Please also indicate your ability and willingness to provide product demonstrations to showcase solution critical functionality.

RFI RESPONSE CATEGORY BREAKDOWN

1. Company overview

1.A. What is your history and experience in providing solutions and services for the cyber security industry?

1.B. Can you elaborate on your company's experience and track record in providing cyber security solutions and services to Defense industries and international organizations such as the EU or NATO?

1.C. What is your experience in providing EDR solutions?

1.D. Please provide any third-party evaluation of your products suite, if available (e.g. MITRE, Gartner, Forrester, …)

1.E. Please indicate relevant regulatory compliance standards or industry standards applicable to your solution or company

2. Solution overview and deployment model

2.A. Please provide an overview of your product suite relevant to EDR functionality.

2.B. What does the system architecture of the solution look like (e.g. use of agents, centralized control, data collection/feeds, …)?

2.C. Does the system architecture allow high-availability / redundancy / load-balancing scenarios within a single site or across multiple sites (e.g. two data centres)?

2.D. What types of platforms and endpoint types does your solution support (e.g. operating systems, mobile devices, …)?

2.E. How does your solution scale, particularly for large dynamic enterprise environments with thousands of endpoints?

2.E.i. What are the central infrastructural requirements regarding total event throughput and data volume regarding the scalability constraints?

2.E.ii. Does the solution allow for on-demand agent deployment on a subset of endpoints as required?

2.E.iii. How is the solution's performance affected by the scaling of the number of endpoints?

2.F. What is the estimated size of the team required to manage the solution?

2.G. Does your solution cover cloud footprints such as Microsoft Azure and Amazon Web Services?

2.H. Does the solution require cloud connectivity? If so, how, and to what extent, does it rely on it?

2.I. Does the solution allow for air-gapped (non-internet connected) and/or hybrid networks?

3. Product features and capabilities

3.A. Can you elaborate on the specific functions that your EDR solution is able to provide?

3.B. What alerting actions does your solution support, and how do you deal with True/False Positive/Negative trade-offs?

3.C. What manual and what automated response actions does your solution support (e.g. user account actions, file actions, network interface actions, …)?

3.C.i. Can the response actions be executed and centrally managed after isolating the client from other network activity?

3.D. What customization does your tool allow for (e.g. custom detection, analysis or response actions)? Please detail the mechanism and available options (e.g. GUI, query language, support for custom scripts/binaries, …)

3.E. How does the solution handle the detection of both known and unknown (e.g. zero-day) threats?

3.F. What forensics capabilities does the solution provide (e.g. types of data, analysis capabilities, workflows, playbooks, …)?

3.G. What are the resource requirements for the solution (per endpoint type, preferably including performance charts)?
  3.G.i. Minimum system requirements
  3.G.ii. Idle resource consumption
  3.G.iii. Typical resource consumption
  3.G.iv. Peak resource consumption
  3.G.v. Ability to limit resource usage
  3.G.vi. Ability to (selectively) offload resource intensive tasks to a central server or a cloud instance?
3.H. What are the correlation abilities or other central analysis capabilities to observe behaviours across multiple (types of) endpoints?
3.I. What are the capabilities of an endpoint agent for analysis/detection and response in case of a disconnected client?
3.J. What endpoint activity does the solution record and use to detect threats? E.g.:
  3.J.i. Process starts, stops, and cross-process injection
  3.J.ii. Network connections
  3.J.iii. File modifications
  3.J.iv. Registry changes
  3.J.v. Binary / executable / application metadata and full content
  3.J.vi. Memory content and structures
  3.J.vii. Others
3.K. Which containment mechanisms are available? Is Network isolation available for both Windows and Linux? Manual isolation of the host through GUI or automatic isolation if certain conditions are met, or both?
3.L. Is the detection logic provided by the vendor open to review/inspection to better understand the behaviour?

4. Data collection, processing and storage

4.A. What types of data can be collected (e.g. users logs, network connections, browsing history, system logs, Kernel logs, OS memory space, …)?
4.B. Can you expand on how data is collected, processed and stored?
4.C. Where can or does the tool do its analysis, including correlations: centralized, in the agent, or both?
4.D. Are there any specific constraints regarding data retention; what parameters can be configured (e.g. time, data size, subset of endpoints, …)?
4.E. What logs are or can be generated in the EDR system itself (e.g. activity logs)?
  4.E.i. Are there features for tracking and documenting actions taken during the incident response process by users/automated playbooks?
4.F. What anti-tampering measures are used to protect the data integrity?
4.G. Can all collected data be retrieved from the solution via an API or otherwise?

5. Threat intelligence and threat hunting

5.A. What are the information exchange methods offered to provide threat information updates to the purchaser teams and the implemented solution?
  5.A.i. What is the frequency of such communications?
  5.A.ii. How are isolated networks kept up to date?
5.B. What threat intelligence feeds are readily supported by the solution (e.g. existing feeds and supported standards such as MISP, STIX or TAXII)?

5.B.i. What are the options for creating custom threat intelligence feeds, importing indicators of compromise (IOCs) and adding new standards?

5.C. What methodologies does your solution employ to detect and identify new threats (threat hunting)?

6. Policy management

6.A. Please explain the different roles available in your solution for policy management hierarchy / delegation model (e.g. central policy definition vs. per site policy application).

6.B. Can you explain the process of centrally managing policies, including dealing with site or endpoint specific deviations compared to a standard baseline configuration?

6.C. How can a user specify custom policies and/or playbooks?

6.D. How does your tool deal with version control of policies? In the case of site or endpoint specific deviations, would changes be overwritten with the next content update?

7. System integration

7.A. Please explain the integration / interfacing capabilities (e.g. API, data formats) of your solution to:

7.A.i. External Identity and Access Management (IAM) (e.g. Microsoft AD)

7.A.ii. External Reporting Systems / Dashboards

7.A.iii. External automation / management systems

7.A.iv. External complementary cyber security solutions (e.g. firewalls, forensic solutions, …)

7.B. How does your solution facilitate integration to external SIEM solutions (e.g. Splunk)?

7.C. How does your solution facilitate integration to external SOAR solutions?

7.D. For all questions above: which of these are supported by default and which require custom connectors?

7.E. Does the solution allow for integration with any of the following tools?

7.E.i. Splunk

7.E.ii. Tenable scanner

7.E.iii. Trellix ePO, ENS, DLP, TAC, MDE

7.E.iv. Fidelis endpoint security

7.E.v. MISP

7.E.vi. Sysmon

7.F. Does your solution support Sandbox integration? If so, does it have native Sandbox available for purchase and integrated with the EDR solution?

8. Tool security

8.A. What security functions and measures are included to protect the system and its data?

8.B. What measures are taken to avoid bypassing or tampering of the system (e.g. hunting on telemetry)?

8.C. Do you have a dedicated team to assess and respond to security vulnerabilities in the product suite?

9. Management

9.A. What is the central management method for the solution?

9.B. What are the management roles to distribute the management privileges?

9.C. Is there a single management console controlling all the solution components?

9.D. Are there functional limitations of the management console that requires use of external interfaces such as CLI?

9.E. What is the compatibility / integration for the management component for on-premises and cloud related modules?

9.F. What reporting capabilities are available for auditing, compliance, and executive reporting purposes?

10. Support, maintenance and service provisioning

10.A. How is the product ensured to be up to date with the latest developments, both functionally and to mitigate new risks?

10.B. What parts of the solution are expected to be operated by the purchaser and which can be provided as a service?

10.B.i. Can you specify what service level guarantees can be provided through these services?

10.B.ii. Are you able to provide any examples of service support models for any managed services that you currently operate?

10.C. What levels and type of support do you offer for the products identified in this questionnaire (e.g. Support Portal; Help Desk 24x7 / 9x5; Technical Account Manager; Development Team access; Onsite Professional Services …)?

10.D. What system diagnostic information needs to be provided with support cases?

10.E. Are you able to provide any guaranteed response and/or resolution times for support cases raised by a Customer?

10.F. What onsite consultancy services are you able to provide (e.g. deployment; integration; configuration, tuning, optimisation; policy management …)?

10.G. Are you able to provide Training on your products and services? If so, in what form (e.g. Face-To-Face at purchaser / vendor site?; Online or CBT; Training material …)

10.H. What are your policies and procedures regarding notification of security vulnerabilities which may be identified in your products (e.g. through internal release testing)?

11. Cost and licensing

11.A. Can you provide a breakdown of your pricing and licensing structure for the EDR solution and related support (per endpoint type, based on number of endpoints, servers, throughput, on-demand scaling, bundles …)?

11.B. Does your pricing model offer a reduced rate for extended contracts beyond one year?

11.C. What are your payment terms?

12. Roadmap and future development

12.A. Can you provide an overview of the relevant near-future product roadmap?

13. Case studies and success stories

13.A. Do you have any recent references and/or success stories that would be relevant that you can/want to share?

13.B. Can you provide a demo environment, workshop, video, or similar, to showcase solution critical functionalities?