סייבר ישראל
משרד ראש הממשלה
מערך הסייבר הלאומי

Israel National Cyber Directorate

Request for Information (RFI)

No. 0305/2023

Subject: Continuous Controls Monitoring (CCM) System

May 2023

Preliminary Request for Information (RFI) for:
Continuous Controls Monitoring (CCM) System

1. Background and purpose of request

1.1 Many organizations use a wide variety of tools to protect their assets, information and IT environment. Continuous monitoring and verification that all the tools are set up and implemented correctly - whether according to the manufacturer's definitions, according to best practices of operation or according to the needs of the organization - are complex operations which consume a lot of time.

1.2 Organizations are required to comply with a set of security regulations and standards (ISO, NIST, PCI, CIS) and a great deal of effort is required to collect and analyze the information originating from the multitude of tools and systems deployed in the organization in order to assess compliance with these standards.

1.3 Organizations need effective methods and tools for assessing the severity of the risk and prioritizing the handling of security gaps of the critical assets involved in their business processes, and so they invest extensive budgets in the purchase of new technologies and protection solutions against emerging threats, yet find it difficult to produce a comprehensive and up-to-date picture of the state of the organization's resilience.

1.4 In light of the above, the Israel National Cyber Directorate seeks to obtain information on CCM (Continuous Controls Monitoring) systems, which are a technological product that continuously monitors the level of compliance with the organization's security controls.

1.5 The product connects to the various security management tools deployed in the organization, such as: AD, FW, EDR, WAF, Vulnerability Management (VM), and for the organization's management tools for the communication infrastructure and systems. It monitors each tool in its field, collects definitions and statuses from each one of the tools and produces a weighted score that reflects the level of compliance with the security defense methodologies, standards or regulations, indicates trends and alerts in cases of irregularities. The product should be capable of dealing with many different types of organizations and an extensive array of security tools.

2 General

2.1 This request is a **preliminary request for information** in accordance with Regulation 14A of the Regulations on the Obligation of Tenders, 1993. It is not intended to establish any type of obligation towards any of the respondents and/or to consider it an agreement of any kind. The request is intended solely for receiving information, and following it the Directorate will consider its subsequent steps in accordance with professional and practical considerations.

2.2 If and when a tender or other procurement procedure takes place in the future, the Directorate will be entitled to change or add conditions and requirements, all according to its professional judgment and according to its needs.

2.3 The Directorate will be entitled to use the information provided to it in response to this request, and the supplier will have no claims related to copyrights.

2.4 Responding to this request will not constitute a condition for participation in the tender, if and when the tender will be conducted following the RFI, it will not grant an advantage in the tender to those who responded to the request just because they responded to it, and will not obligate them to participate in the tender or agree to it in any other way.

2.5 You can view and download the complete documents of the request for information that are available on the website of the Government Procurement Administration at: https://www.mr.gov.il/Pages/HomePage.aspx or on the website of the National Cyber Directorate at: http://cyber.gov.il.

2.6 Below is a table listing all the dates for this RFI:

Action	Date	Hour
Date of publication of the RFI	15.5.23	14:00
Deadline for submission of clarification questions by the suppliers	29.5.23	12:00
Deadline for the Ministry's response to the clarification questions	7.6.23	12:00
Deadline for submitting responses	15.6.23	12:00

3 Basic Concepts:

3.1 CCM (Continuous Controls Monitoring) system - a technological product which continuously monitors the level of compliance with the organization's security controls.

4 Requirements specification

As part of this RFI, the Israel National Cyber Directorate (hereinafter: "**the Directorate**") requests information about systems that provide a solution according to the following, as detailed below.
It is hereby clarified that the requested solution is intended to be integrated into organizations with different characteristics in the market (infrastructure, industrial entities, etc.), according to the needs and characteristics of the organization, and to be adapted for connection to different types of components - OT, IT, IOT components, etc.

4.1 **The respondent will detail the capabilities of the product / system with reference to the following aspects:**

4.1.1 Is the service SaaS?

4.1.1.1 Does the bidder have the ability to operate the service based on the cloud infrastructures selected in the Nimbus tender (Central Tender 01-2020 for the provision of cloud services on a public platform for government ministries and auxiliary units), AWS or GCP and can the bidder establish, in the Israeli region, a data center of the cloud infrastructures selected in the Nimbus tender in order to provide the service from this center?

4.1.1.2 If the answer is negative, how long will it take to set up the service as described above?

4.1.1.3 You can learn about the government's requirements in terms of cyber security, privacy, terms of use, storage and processing of information, as well as additional requirements in terms of information security in relation to working in the cloud, which the proposed solution is required to meet, in accordance with the details in the central tender for adding services to the government digital market in the cloud, which was conducted as part of the Nimbus project and its documents are published on the Procurement Administration website at the following link:

https://mr.gov.il/ilgstorefront/he/p/4000553566

4.1.1.4 The CCM (Continuous Controls Monitoring) system will automatically and continuously examine the correctness of the Cybersecurity Controls settings and controls implemented in the monitored organizations.

4.1.1.5 Examining the existence of known vulnerabilities in software or system components such as CVEs.

4.1.1.6 The system will contain built-in recommended cyber protection settings in accordance with accepted standards in the market, such as NIST, ISO-27001 as well as manufacturer settings and/or best practices.

4.1.1.7 The system will allow the user to update (add, change or cancel) the security settings mentioned above according to the security policy that he needs to implement and measure.

4.1.1.8 Management interfaces

4.1.1.8.1 Management interface for a group of organizations - an interface that allows viewing, setting and updating of controls and monitored systems for a group of organizations

4.1.1.8.2 Management interface for an individual organization - an interface that allows viewing, setting and updating of controls and monitored systems for a single organization

4.1.1.8.3 The system will contain interfaces (such as APIs) for monitoring common IT and/or ICS (OT) management and security products, belonging, at least, to the following product families. The respondent will list the relevant systems in each of the following families:

4.1.1.8.3.1 Asset Management / Identity Management

For example: Microsoft Active Directory, BigFix, SCCM

4.1.1.8.3.2 Firewall

For example: Checkpoint, Fortinet, Cisco, Palo Alto

4.1.1.8.3.3 IPS (Intrusion Prevention Systems)

For example: TrendMicro, Cisco

4.1.1.8.3.4 AV & EPP/EDR

For example: VMware Carbon Black, Symantec, McAfee

4.1.1.8.3.5 Email Gateway

For example: Microsoft, Symantec, TrendMicro

4.1.1.8.3.6 Virtualization

For example: VMware vCenter, Microsoft Hyper-V

4.1.1.8.3.7 Patch Management

For example: HCL BIGFIX, Microsoft WSUS

4.1.1.8.3.8 Vulnerability Management / Assessment

For example: Rapid 7, Tenable

4.1.1.8.3.9 Vulnerabilities Scanners & BAS (Breach and Attack Simulation)

For example: Rapid 7, Nessus, Skybox, Pentera

4.1.1.8.3.10 WAF & Load Balancer

For example: F5, Imperva

4.1.1.8.3.11 NAC

For example: Forescout, Portnox

4.1.1.8.3.12 VPN

For example: PulseSecure, Fortinet

4.1.1.8.3.13 Network / Network Management

Various network components (routers, switches, etc.)

4.1.1.8.3.14 DB

For example: MySQL, SQL Server, MongoDB

4.1.1.8.3.15 Cloud

For example: Azure, AWS, GCP

4.1.1.8.3.16 Storage

For example: Dell EMC , NetApp , Veeam

4.1.1.8.3.17 Legacy Systems

For example: SAP, Net and Oracle, Lotus Notes

4.1.1.8.3.18 OT-IDS

For example: Fortinet, Splunk, Checkpoint, Tenable OT

4.1.1.8.4 The monitoring of the various systems will be carried out in a way that does not harm or impair the performance of the systems being tested. The monitoring will be based on importing/collecting data from the systems using the API interface or exporting, using legitimate commands, of the settings of the systems being tested.

4.1.1.8.5 Adjustment of the above interfaces, without code changes, through configuration.

4.1.1.8.6 Adding new interfaces (SDK).

4.1.1.8.7 Views via the system portal and/or reports:

4.1.1.8.7.1 Displaying data continuously and in real time.

4.1.1.8.7.2 The Cybersecurity Posture status, including a weighted risk score, taking into consideration the severity/importance of the monitored controls, for the entire organization, and divided into the monitored product families (according to the above list).

4.1.1.8.7.2.1 The normal operation of the monitored systems.

4.1.1.8.7.2.2 Implementation of cyber security controls in these systems in accordance with the standard chosen to serve as the basis for monitoring.

4.1.1.8.7.2.3 Detailing that explains the nature of the control, its effect on the security level of the system and the correct way to implement it or to implement a compensatory/alternative control.

4.1.1.8.7.2.4 Score and rating of the severity and importance of each control based on accepted manufacturer recommendations or another severity standard accepted as a basis for compliance.

4.1.1.8.7.2.5 Pointing at gaps and recommendations for correcting and improving the existing situation.

4.1.1.8.7.2.6 Updating the standard used as a basis for compliance.

4.1.1.8.7.2.7 Changes in the security overview over time, including alerts on deviations from expected behavior, of the entire organization, of a family of products or of a specific product.

4.1.1.8.7.2.8 Support for displaying the above status overview in a concentrated manner, in several hierarchies:

4.1.1.8.7.2.8.1 At the organization level and for complex organizational structures (Multi-site, International, etc.)

4.1.1.8.7.2.8.2 A sector status overview consisting of the weighting of the overviews of the monitored organizations that comprise it.

4.1.1.8.7.2.8.3 A national status overview consisting of the weighting of the overviews of the total number of monitored organizations.

4.1.1.8.7.2.9 Support in displaying the above situation overview, in different hierarchies, to different stakeholders, including: the operation team (SOC/NOC), the IT Infrastructure Administrator, the CISO, the Risk Officer, Supervisor of an organization / sector in the

Israel National Cyber Directorate, a National overview of the situation (total monitored organizations).

4.1.1.8.7.2.10 The system has the ability to perform data filtering and display the test results according to the type of system being tested, the name of the organization / network, as well as customized divisions/classifications, such as a number of organizations that the central client (the Israel National Cyber Directorate) assigns to the same group.

4.1.1.8.7.2.11 The system will allow the generation of reports in a variety of common formats such as PDF, Word, CSV.

4.1.1.8.7.2.12 The system will support the ability to build a template of controls according to the specification of the central customer. It is required to detail the impact of building a customized template for the client on the reports, data filtering, and more.

4.1.1.9 Role based access control (RBAC) including reference to the different types of users (administrator, manager of a group of organizations, representative of a monitored organization), to the various display hierarchies (as mentioned above), and the ability to define the viewing of information according to access permissions.

4.1.1.10 The ability to adapt the system to different organizations - size, classification (unclassified, classified, operational) and network structures - air-gapped / connected.

4.1.1.11 The settings of the tested systems will be saved in a secure / encrypted manner in the testing system, or alternatively will not be saved at all and will be analyzed by the CCM system in an online configuration.

4.1.1.12 The system has a capacity for wide coverage over several organizations and networks, of collection agents and the capability of transferring the collected data to a central server for analysis.

4.1.1.13 The transfer of data from the collection agents to the central server will be carried out in an encrypted manner that is secure against eavesdropping and interference.

4.1.1.14 The central server for data analysis will be installed in a secure On Prem environment and/or in a cloud provider according to the central customer's requirement, in one of the two cloud providers that won the Nimbus tender.

4.1.1.15 It is required that the central server will enable the saving of data to be analyzed in a secure and encrypted manner.

4.1.1.16 It is required that the central server be managed by the central client or by another client on its behalf (for example, a sectorial unit) in full, while controlling the access privileges, and that the provider will have access solely for support purpose, under the control of the central client and his knowledge.

4.1.1.17 In addition to the requested response as detailed above, respondents may present additional and/or integrated capabilities and services as well as existing and future concepts and ideas.

4.1.2 <u>The respondent will list the details of the respondent company:</u>

4.1.2.1 Is the responding company the company that develops the product/system and its owner?

4.1.2.2 Is implementation and support for the product/system provided directly by the responding company? If not, who provides the implementation and support?

4.1.2.3 Does the responding company have a development and/or support center in Israel?

4.1.2.4 How many paying customers does the product/system have?

4.1.2.5 Are some of the clients listed above financial and/or government clients? If so, how many are they and are they located in Israel? For how many years?

4.1.2.6 How long has the product/system been on the market, used by the paying customers listed above, in Israel and around the world?

4.1.2.7 What is the pricing model, referring to the content of a license to use the system:

4.1.2.7.1 How many and which tools are included in the user license?

4.1.2.7.2 How many organizations are included in the user license?

4.1.2.7.3 Are there pricing levels for different amounts of user licenses?

4.1.2.7.4 Are there any other services that are not included in the license, and what is their price?

4.1.2.8 If at least the answer to one of the two sections, concerning the operation of the service based on the winners of the Nimbus tender and a data center in the Israeli region, is negative, what is the cost of implementing the operation of the service in this manner? If this issue is a condition for providing the service to government offices in Israel, what is the solution proposed by the respondent?

4.1.2.9 How are development hours priced with reference to dedicated tasks and complete projects?

4.1.2.10 How are Professional Services (PS) hours priced?

4.1.2.11 Is it possible to price a project for interfacing the service with systems and portals that are external to the service according to the customer's requirements and what is the pricing mechanism?

4.1.2.12 Is it possible to price a development project according to the customer's requirements and what is the pricing mechanism?

4.1.3 Are there any documents detailing the terms of use of the service and terms of agreement? If so, please attach them.

4.1.3.1 The respondent may add any additional relevant information relating to these topics.

5 Requested response

The proposals must provide a response that refers to each of the requirements listed in section 4 above, including reference to the following issues:

5.1 For all proposals:

5.1.1 Presentation of capabilities as specified in section 4.

5.1.2 Proposing solutions with the ability to adapt to different organizations - size, classification (unclassified, classified, operational) and open / closed network structure.

5.1.3 Ease of installation, operation and updating.

5.1.4 Proposals or ideas regarding the establishment of the infrastructures, tools or systems required to fulfill the requirements from the proposed system.

5.1.5 In addition to the requested response as detailed above, respondents may also present existing and future concepts and ideas, as well as additional services that expand the overall response.

6 How to submit clarification questions and responses to this request

6.1 Contact person

The contact person on behalf of the Directorate regarding this request is Sharon Bousidan, phone 072-3388578 email cyber-michrazim@cyber.gov.il

6.2 Clarification questions

6.2.1 Clarification questions regarding this request must be submitted in writing only, no later than the deadline for provision of clarification questions as detailed in the table in section 2.6, to the contact person, by email cyber-michrazim@cyber.gov.il. The supplier must make sure that his questions have reached the contact person, at 072-3388578.

6.2.2 The Directorate reserves the right to conduct one or more rounds of clarification questions at its sole discretion.

6.2.3 The clarification questions will be submitted in Hebrew, in the following structure:

Number of the section in the request	Question

6.2.4 Answers to the clarification questions will be forwarded by the Directorate to the applicants, and will also be published on the website of the Government Procurement Administration and the National Cyber Directorate at the addresses specified in section 2.5 above. It is clarified that the clarification answers will be worded in a way that does not reveal the identity of the questioners.

6.3 Submission of a response to the request

6.3.1 The response to the request will be submitted **in Hebrew or English**, and will total up to 50 pages that present the response. In addition to this, appendices and technical specifications can be attached without a scope limitation.

6.3.2 The answer to the request for information must be submitted in a digital copy by the deadline for submitting responses, as detailed in the table in section 2.6 above, via an email box Cyber-Michrazim@cyber.gov.il. Receipt must be confirmed at Tel: 072-3388578. The email's subject line will be: "Preliminary request for information (RFI) on the subject of "Continuous Controls Monitoring (CCM) System".

6.3.3 The Directorate may postpone the deadline for submitting a response at its sole discretion. A notice of this will be sent to everyone who responded to the request, and will also be published on the websites of the Government Procurement Administration and of the Directorate, at the addresses specified in section 2.5 above. The notice will indicate the new date for submitting the responses.

6.3.4 As part of the response, the respondent will provide the following information:

No.	Requested information	Response
1	Respondent's name	
2	Respondent's address	
3	Phone Number	
5	Name of contact person for respondent	
6	Contact person's phone number	
7	Contact person's email	

7 Examination of the response

7.1 The Directorate reserves the right to contact, as necessary, the respondents with requests for information and clarifications, for presentations and demonstrations, for visits to the client's sites and the sites of those who responded to this request, at the discretion of the Directorate.

7.2 As part of the examination of the responses, the Directorate reserves the right to invite any respondent to present the solution proposed by him to a professional team on his behalf at a location and at a time determined by the Directorate.

7.3 As part of the examination of the responses, the Directorate reserves the right to invite the proposers to hold a pilot that will last up to two months long. It is hereby clarified that the Directorate reserves the right to invite only some of the proposers to hold the aforementioned pilot, at its sole discretion, according to the needs and capabilities of the Directorate and the availability of the proposers.