Artificial Intelligence (AI) Driven Cyberspace Security Continuous Monitoring System (AIDCMS)

18 October 2023

Submission Close

24 September 2023 11:59 PM ET

U.S. Citizens Only

Purpose

The Cyber Fusion Innovation Center (CFIC), in collaboration with U.S. Army Cyber Command (ARCYBER) and Army Cyber Technology and Innovation Center (ArCTIC) invites qualified industry partners to submit proposals for the design, implementation, and maintenance of an AI-driven Cyberspace Security Continuous Monitoring System. Our organization seeks to enhance security posture, enable resilience in Army operations, and preempt evolving cyber threats.

Background/Synopsis

U.S. Army Cyber Command operates and defends Army networks and delivers cyberspace effects against adversaries to defend the nation with over 16,500 Soldiers, civilians, and contractors working 24/7 across the globe. In today's rapidly evolving threat landscape, we recognize the importance of continuous monitoring as a foundational component of our cyberspace security ecosystem. The Army requires the ability to automatically and continuously monitor systems to maintain ongoing awareness of information security, vulnerabilities, and threats to facilitate risk-based, operational decision making. Automation is required to analyze the high volume and variety of data elements associated with successful continuous monitoring. Because of functional drift, monitored systems analytic thresholds and weights must be automatically updated to reduce the likelihood of false positive alert notifications, and accurate indication of anomalous or malicious cyber activity.

Scope of Work and Deliverables:
The selected Industry Partner will be responsible for:

1. Designing, implementing, and sustaining a comprehensive AI-driven Cyberspace Security Continuous Monitoring System that can execute two primary functions:

A. Function 1: Parse monitored system artifacts such as EMASS scans (typically from ACAS) and network maps as inputs to generate a risk-based prioritized list of log events that can be analyzed to detect anomalies and threat activity related to the five core categories listed below (as outputs). The generated list should articulate prioritization and categorization of the events to be analyzed and formatted for function two ingest and prosecution. For example, if the monitored system consists of windows hosts and servers', function one would generate a list of events that should be monitored in order to detect activity that meets the criteria in the five categories listed below.

B. Function 2: Connect to monitored system SEIM, API or File System and analyze log events specified in the outputs above to detect and report anomalies, malicious behavior, and change detection over a period within the five core threat activity categories listed below. At detection, disseminate confidence-bound time sensitive alerts and periodic reports that describe the detected activity while periodically updating analytic thresholds and model weights. Near real-time adjustment for the monitored systems functional drift (which includes drift of AI model(s) and underlying data distribution shift) should occur over a defined period.

2. Five threat detection activity categories: The Continuous Monitoring capability must be able to detect anomalous activity and categorize malicious activity. Detections must include confidence ratings to quantify uncertainty of estimations related to the following activities by analyzing the monitored system logged events as specified in Function one for function two ingest and prosecution.

A. Initial Access: Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a monitored system.

B. Lateral Movement: Lateral Movement consists of techniques that adversaries use to enter and control adjacently positioned, remote systems on a given networked architecture.

C. Malicious Command and Control (C2): Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network.

D. Illicit Data Exfiltration: Exfiltration consists of techniques that adversaries may use to steal data from the monitored system and egress the data across the network.

E. Credential Theft or Misuse: This consists of techniques for stealing credentials like account names and passwords and giving them access to systems, making adversary activity harder to detect.

3. Integrating threat intelligence feeds to enhance threat detection capabilities.

Monitored System Scope:

1. The monitored systems will consist of enterprise information technology (IT). The continuous monitoring system must analyze event logs consistent with IT systems such as Linux and Windows client and server hosts, Antivirus, NetFlow and DNS.

2. The continuous monitoring system will connect to the monitored systems event log repository/SEIM remotely via API (e.g., S3 Bucket, Elasticsearch, Splunk query).

Performance Thresholds:

We expect the proposed system to achieve the following performance thresholds:

1. Detect known malicious activity within the five categories listed above with an overall effectiveness of 70% using a documented statistical confidence bound. When using AI, Machine Learning models, or algorithms affirm an F1-score of at least 50% and documented statistical bound for detected anomalous activity within

the five categories. All performance thresholds should convey a documented false-positive minimization approach.

2. Alert Generation: Generate risk-based, prioritized alerts within five minutes of identifying a potential threat or incident within the five-core threat detection categories specified above. Alerts must be transmitted securely via email or an approved communication technology.

3. Report Generation: Generate at least two periodic summary reports focused on activity related to the five threat categories listed above. Generate a 24-hour, 7-day and optionally 30-day coverage report that describes monitored system activities highlighting anomalous or malicious activity that was alerted to during the previous reporting period. The report should also contain details describing the activity of the note that did not meet the threshold of alerting but was of significance. The report should summarize activities that may span multiple monitored environments in a single report.
4. Scalability: The system should accommodate the ability to scale the continuous monitoring system to monitor multiple systems while periodically updating analytic thresholds, model weights and maintaining optimal performance.

5. System Uptime: Ensure a minimum system uptime of 90% while describing how you would address redundancy and failover mechanisms. Describe system uptime percentages during model re-training, system maintenance, and in various degraded state operations.

6. Integration Capabilities: Describe, at a high level, how your proposed system would integrate with our existing security infrastructure, tools, and platforms (e.g., reporting, and ticketing systems).

7. Threat Intelligence Utilization: Leverage threat intelligence sources to enhance threat detection accuracy by at least 20%. Define the baseline and methodology applied to determine threat detection accuracy above 20% to affirm consistent measurement.

8. Describe how this system will be deployed globally and what impact on measures of effectiveness may be incurred.
U.S. Army Cyber Command operates and defends Army networks and delivers cyberspace effects against adversaries to defend the nation with over 16,500 Soldiers, civilians, and contractors working 24/7 across the globe. In today's rapidly

evolving threat landscape, we recognize the importance of continuous monitoring as a foundational component of our cyberspace security ecosystem. The Army requires the ability to automatically continuously monitor systems to maintain ongoing awareness of information security, vulnerabilities, and threats to facilitate risk-based, operational decision making. Automation is required to analyze the high volume and variety of data elements associated with successful continuous monitoring. Because of functional drift, a monitored systems analytic thresholds and weights must be automatically updated to reduce the propensity for false positive alert notifications while accurately indicating when anomalous or malicious cyber activity occurs.

Why You Should Participate

ARCYBER seeks to enter into non-FAR or FAR-based agreements with Industry, Academia, and National Lab partners whose solutions are favorably evaluated by ARCYBER Subject Matter Experts (SMEs). As such, the follow-on Assessment Event (AE) is considered competitive, and solutions will be evaluated independently of one another primarily for technical merit. This serves dually as notification of the intent to research the feasibility of an agreement under 10 U.S. Code, Section 4022 and/or Section 4022(f), and as notice of pre-solicitation activities IAW FAR 5.204.

Event Timeline

Phase 1 – 9 June - 25 July 2023 Collaboration Event RSVP Window:
Confirmed Government partners will identify current limitations and ideate ways to overcome limiting factors. Problem statement(s) will be developed to frame automated continuous monitoring needs. Outcomes from the Collaboration Event will shape the Industry, Academia, and Laboratory Assessment Event, date TBD.
COMPLETED

Phase 2 – 8 August 2023 Industry, Academia, and Lab Collaboration Event: CFIC will host the Collaboration Event (CE) with Industry, Academia, and Laboratory partners focused on AI for Continuous Monitoring. During this event, Warfighters will interact with potential solution offerors and further communicate operational needs and desired outcomes. Participation in this event is not mandatory, however, it is designed to provide insights to ensure potential offerors understand the problem set(s) fully and to increase the likelihood of matching their technologies

with Warfighter needs. This CE is also an opportunity for attendees to meet and form partnerships that may provide a more comprehensive solution. You will be able to submit your solutions at the follow-on assessment event. **COMPLETED**

Phase 3 – 17 August – 24 September: Assessment Event Submissions to the Assessment Event Open: Interested respondents who could potentially provide solutions that meet the needs of ARCYBER are encouraged to submit their capability for ARCYBER review.

Phase 3a – 7 September 2023: Q&A Telecon: Interested offerors may participate in a virtual Q&A session to better understand the specific technology objectives. The telecon will take place on 7 September from 2:00 – 4:00 PM ET. RSVP form will be available on or around 21 August.

Phase 4 –9 October 2023 Down-select: ARCYBER will down-select those respondents/submissions they feel have the highest potential to satisfy their technology needs. Favorably evaluated submissions will receive an invitation to attend the AE on or around 3 October.

Phase 5 – 18 October 2023 Assessment Event (AE): During the AE, selected participants will be allotted a one-on-one session with the ARCYBER evaluation panel to pitch, demonstrate, and/or discuss their solutions. The forum will include a Q&A portion and discussions may continue outside of the event. Solution brief presentation guidelines will be outlined in the event invitation and solutions will be assessed according to the criteria in the link provided below. If the ARCYBER evaluation panel favorably evaluates a solution brief, negotiations for Phase 6 may immediately begin.

This event will be virtual only.

Phase 6 – Path Forward: Successfully negotiated awards may fall under any combination of these categories:

- Business-to-business research and development agreement as a sub-award through the CFIC Other Transaction Authority (OTA) for research or prototype projects (10 U.S. Code Sections 4021, 4022)
    - An award under 10 U. S. Code, Section 4022 may result in the further award of a follow-on production agreement

without additional competition based on successful prototype completion. The Government may make this follow-on production award even if all successful prototype criteria are not fully met during the prototype project.

- Procurement for experimental purposes (10 U.S. Code Section 4023)
- Cooperative Research and Development Agreement (15 U.S. Code Section 3710a)
- Prizes for advanced technology achievements (10 U. S. Code Section 4025) and/or prize competitions (15 U.S. Code 3719)
- FAR-based procurement contract

How You Can Participate

1. Submit to the call in Vulcan here.
2. Download Vulcan submission instructions here.
3. Download white paper template for submission here.

Questions?

AIDCMS Q&A Telecon Transcription of 7 September Virtual Meeting: https://bit.ly/3PIT1vH

For event-related questions, please contact Brandon Sizemore at bsizemore@cyberfic.org and Mary Burnette at mburnette@cyberfic.org

DISCLAIMERS:

An award under 10 U. S. Code, Section 2371b may result in award of a follow-on production in accordance with 10.U.S.C. 2371(f). Upon a determination that the competitively awarded prototype project(s) have been successfully completed, and subject to the availability of funds, the prototype project(s) may result in the award of a follow-on production contract or transaction without the use of competitive procedures. Such awards may include multiple phases.

Non-Government advisors may be used in the evaluation of submissions and will have signed Non-Disclosure Agreements (NDAs) with the Government. The Government understands the information provided in this announcement is presented in confidence and may contain trade secret or commercial or financial information and agrees to protect such information from unauthorized disclosure to the maximum extent permitted and as required by law. An organization's participation in any part of the selection process under this announcement indicates concurrence with the aforementioned use of contractor support personnel.