AI ATAC3 Frequently Asked Questions (FAQs)
Updated 1/14/2021

Questions asked of the AIATAC.PRIZE.CHALLENGE email alias will be collected and answered by the appropriate persons. The questions and answers will be shared with all formal participants on Challenge.gov and via email, so all participants receive the same information at the same time. Also, details of AI ATAC challenges 1 and 2 can be found by searching on the Challenge.gov page, and many answers are within the AI ATAC3 rules, including the link to the White Paper.

Answers given as "TBD" are being worked by the technical staff, and an answer will be provided when their analysis is complete.

Question 1. "[o]ne thing we noted in the instructions is the on-premise / disconnected scenario. We do not have a version currently for a completely disconnected environment. Would this still be an entry that would be of interest?" Also, "Our solution that goes beyond SOAR is a 100% cloud based solution and meets the requirements with the exception of the on-prem portion. Will our solution that requires internet access be permitted for consideration?" and "Some of the concerns we have center on the boundaries of the challenge, namely that cloud access isn't allowed during the challenge."

Answer 1: The primary goal of this challenge is to run software tools within DoD/DON SOCs to enhance the efficiency and effectiveness of security analysts. As the DoD moves forward, it will be considering how it moves to a greater usage of the Cloud, both commercial and military. For AI ATAC 3, submitted technologies will be allowed to use the Cloud, via the Internet, to run their software during this challenge. We expect this to facilitate checking of license keys, checking and updating threat databases, running portions of the code remotely on vendor systems, and so on. However, NAVWAR and ORNL may be running portions of the challenge in a D-DIL (denied, degraded, intermittent, or limited) environment, to determine the impact of D-DIL on the effectiveness of the tool and the operators running it.

Q2. "Our solution has functionality beyond just SOAR as that is a piece of our integrated platform, if all aspects of our technology are demonstrated within the video presentation be acceptable? With a focus on the SOAR capability."

A2: Yes. We allow you to showcase any aspects of your tools that you wish in your video, so long as you stay within the time limit.

Q3. "Will additional questions be accepted and answered after Jan 22th?"

A3: Yes. Questions will be accepted until 12 February 2021, when submissions are due.

Q4. "How many submissions will be chosen for down selection for Phase 2?"

A4: This will be based on the number of submissions and the extent to which submissions meet the specified criteria.

Q5. "In Phase 2, What types of log sources will be utilized within the SOAR Challenge?"

A5: An important ability for SOAR tools is the ability to integrate flexibly with a variety of data sources. Log sources will generally be those used by DoD systems administrators and cyber analysts. Please note that some representative sources are listed in the AI ATAC3 Challenge.gov web page.

Q6. "In Phase 2, What products will be available within the testing environment to interact with?"

A6: See Question 5.

Q7. "In Phase 2, Will there be an Active Directory structure that can be tied into?"

A7: An Active Directory structure will be used in the test network.

Q8. "How long after phase 2 starts will a winner be notified?"

A8: The length of the competition will be determined in part by the number of participants.

Q9. "When and How is the prize money to be released after the winner is notified?"

A9: Upon determination of a winner (if any), the NAVWAR financial office releases the funds to the winning company. This process can take a few weeks.

Q10. "Can we use our own pre-determined detection sources (e.g. endpoint + email + cloud) or will the sources be of the government's choosing?"

A10: Detection sources will be of the Government's choosing.

Q11. "What mix of log vs. alert sources will it be?"

A11: Specific details as to the nature of the testing will not be revealed.

Q12. "Can we use a non-production version of our software to show 'unique capabilities' coming soon?"

A12: Yes. You are encouraged to submit the solution that you think will perform the best in the competition. However, the goal of the competition is to find a solution that can be obtained for operational use within Navy networks.

Q13. “Are there any specific requirements on the on-prem version separate from the Cloud?”

A13: TBD.

Q14. “What are the specific technologies (Vendor) that will be used to generate logs & alert data?”

A14: Please see answer #11.