# AI ATAC3 Questions and Answers

# Updated 1/27/2021

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. The latest questions, and any changed questions, are at the top of this document, for ease of finding the most up-to-date information.**

Question 22. “How are data feeds and logs delivered to the tool (how is the tool supposed to ingest data feeds)”

Answer 22. Logs and alerts will be forwarded from the network’s hosts and servers in two ways: (1) directly to the submitted SOAR tool, and (2) to a provided SIEM (already on the network) and then to the submitted SOAR tool. The submitted SOAR tool must accept logs from the provided SIEM.

Logs and alerts from standard network sources (for which many SOAR tools promise native integrations) and from custom sources (for which no SOAR tool provides native integrations) will be tested. The submitter’s user / setup guide must provide instructions on how to configure the SOAR submission to ingest data for these situations.

Q23. “What is the exact format of data ingest? a. Can we get an example? b. Is the data raw, parsed?”

A23. Standard and custom alerts and logs from SIEM tools and other host and network sources will be used. Examples of standard formats include .csv, .json, and syslog. This is not an exhaustive list.

No sample data will be provided.

Reference Answer 22 above.

Q24. “Can you share an available dataset to train machine learning models?”

A24. No.

Q25. “What are high-frequency tasks for junior analysts?”

A25: Responding to alerts, data gathering, performing case management, recommending solutions, reviewing logs, coordinating with other analysts, elevating an incident to senior analysts, associating/correlating data from multiple sources, documenting incidents and responses, reviewing and updating dashboards, opening, working, closing tickets, running and potentially editing playbooks. This is not an exhaustive list.

The list of tasks under “Description” on the AI ATAC3 Challenge web page lists some representative activities.

Q26. “Do we need to store original logs? How long do logs need to be stored?”

A26. A SIEM will be provided on the network. Whether or not a particular submission needs to store logs is up to the submitter. If storage time requirements are needed, up to 6 months.

Q27. “What tasks do analysts need to collaborate on (real-time collaboration)?”

A27. Collaboration will occur in areas ordinarily associated with SOAR tools: sharing and updating tickets, sharing and updating playbooks, handing off an incident, e.g., from a junior analyst to more senior analysts. Coordination of tasking and consolidating results.

Q28. “What ticketing system is used within the SOC?”

A28. To Be Determined (TBD)

Q29. “Does the submission have to be mailed? If so, can it be post-marked by the deadline?”

A29. The submission does not have to be mailed, a complete submission can be sent via email. Regardless, per the challenge rules, submissions must be received no later than 12 February 2021 at 1700 EST. Please coordinate with the AI ATAC email alias on best method and address to email the submission.

## Prior Questions

**No changes to questions below since the 1/21/2020 FAQ document was promulgated**

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.

Answer 1 (continued) To clarify this issue further, the following words will be put into the AI ATAC3 rules. This update does not change the intent of the challenge: vendors are encouraged to propose whichever sort of solution they believe will meet the rules most effectively. However, tools may be tested in a D-DIL environment in which connections to the Internet or the Cloud may be degraded or denied. The exact verbiage is below:

* **Cloud and On-Premises (On-prem) Requirements:** For testing, submitted technologies will be installed on the Cybersecurity Operations Research Range (CORR) evaluation environment at Oak­ Ridge National Laboratory (ORNL). Due to the potential variety of solution types, the Challenge will accept solutions that require access to external resources as well as solutions that are hosted on-prem. 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 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.

As such, during a portion of the testing, no connection to the Internet or an external Cloud should be expected, and all technologies and licenses will be evaluated as to their ability to function without connectivity to a Cloud environment or the Internet.

During a portion of testing, ORNL will test the ability of the submitted technology to facilitate collaboration of SOCs on different networks using their own instances of the SOAR tool. All networks will be inside CORR (ORNL’s testbed). To test interaction of the SOCs/SOAR tools across networks, there are two options, as follows:

* + - Internet connections will be provided to enable connections to the Cloud. Cloud provision and configuration must be provided by the submitting team if this option is used. (SOC-A talks to SOC-B via an external connection.)
    - Solutions that do not require external Cloud access, but do allow coordinating across connected networks within ORNL’s testbed are permitted, in lieu of Cloud connections. This simulates connecting multiple SOCs all on a separate enclave, e.g., SIPRnet. (SOC-A talks to SOC-B directly on an internal network.)

The submitter should select the tools and configuration that they believe will best meet the Navy’s need, whether that solution uses a private Cloud, virtual Cloud, an on-prem solution, or some combination of them. The important necessity is that multiple networks with different instances of this SOAR tool must be able to collaborate either using a remote capability (Cloud or external Internet) or via an ORNL-on-prem capability (internal, private networks).

Regardless of the proposed solution type, all necessary components (software, licenses, configuration / setup instructions, and potentially hardware) must be provided by the submitter. ORNL will allow external access to resources such as the Cloud, however, it will not provide external Cloud resources, either commercial or Government.

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: Please see the revised answer to Question 1.

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

A14: Please see answer #11.

Q15. “Is this a SOAR focused opportunity or are you pulling this opportunity under the SOAR profile as a broad profile?”

A15. This is a SOAR focused opportunity, however if a solution meets the requirements it will be considered. The competition is for functionality, not merely a particular category or name of software. Please see the definition of a SOAR tool on the Challenge.gov page.

Q16. “Should we partner with a SOAR solution to provide the playbooks? We do not provide those but can integrate with others.”

A16. We cannot recommend how to submit your tool or solution. If you have the capability of providing a solution or tool that integrates well with your own, you are welcome to submit it. However, the testing analysts will not perform systems integration for multiple components. The Challenge rules also state, “As part of its submission, Participants must either own the intellectual property (IP) in the solution or provide documentation that indicates all IP stakeholders in its submission. The documentation should describe the type of IP and the entity that holds title to the IP. In either case, only one entry for each commercial technology is allowed.” Playbooks or workflows are a critical component of this Challenge as laid out in the rules.

Q17. “We are interested in participating in this if this maps, what is the process?”

A17. Please follow the submission rules posted on Challenge.gov

Q18. ‘The challenge document states "...only one entry for each commercial technology is allowed." Can a technology, like an XYZ (redacted), which is not a stand-alone SOAR solution, but can add value to any SOAR solution, be bid by multiple different bidders? ‘

A18. If the third-party solution that “can add value to any SOAR solution” is open source, e.g., Zeek network data analyzer, then any and all submissions may use it. If the aforementioned third-party solution is not open source, and the intellectual property (IP) is not owned by the submitting party, a letter of consent is needed from the owner of the IP (presumably the third-party). In both cases (open source or proprietary solution), the answer is “Yes”. However, details of the third-party tool and how it is used must be discussed in the whitepaper portion of the submission. All submissions must work “out of the box” without requiring the integration of disparate components.

Q19. “Can we provide hyperlinked text in the response and/or raw links?”

A19. Yes, so long as the material is readily available for download and easily associated with the submission. Stipulations as to page limit and video length are still applicable.

Q20. “Is a download link sufficient for the software? Or does it need to be included on digital media in the submission package?”

A20. A download link is sufficient.

Q21. “Are web links to online documentation for installation instructions sufficient? Or does a printed copy of the installation instructions need to be included in the submission package?”

A21. A download link is sufficient.