RFI: **RFI-ACT-SACT-22-130 - NATO Classified Cyber Range (NCCR)**

Reference: Q & A

Date of Issue: 18 October 2022

The following questions were raised with respect to subject **RFI-ACT-SACT-22-130 - NATO Classified Cyber Range (NCCR)**. Responses are to provide clarification.

Questions	Responses
1. Is there a specific geographic location for the users of the platform or are they dispersed?	1. There is no specific geographic location for the users. For the use of the NCCR three different scenarios are possible. • Classroom right next to the NCCR, in a secure physical environment. • Users should be able to connect to the NCCR via an encrypted point-to-point connection • Users should be able to connect to the NCCR via NS-WAN (only if feasible)
2. With respect to physical architecture, does NATO wish for the respondent to provide physical hardware if it is not part of the proposed solution? (e.g. access or hosting devices such as desktops, laptops, servers)	2.No. At this stage, it is not necessary to provide any hardware.
3. 3.2 states inbound data only, while 3.5 seems to imply inbound and outbound data exchange. Can you clarify desired directionality of traffic	3.Physically, the NCCR will be connected to NS-WAN. In order to insert non-classified information a unidirectional connection from UNCLASS to CLASSFIED shall be implemented. Within NS-WAN are different data-sources, which will provide information for the NCCR (current threats, intel reports, etc.).
4. With respect to 3.7, will NATO be providing training curriculum or is respondent required to develop this material to execute?	4.Training will be developed by NATO, following the Global Programming framework. Industry support might be needed to develop the training; however, this is not part of this RFI.
5. With respect to 3.8, what is NATO's desired data retention policy? How long does data need to be archived for?	5.This depends on the final solution and is not part of this RFI. In general, the mission/exercise data should be stored as long as possible, but at least as long as all Lessons Learned are developed and tested/implemented.
6. Survey question 4, is commercial cloud provider infrastructure available via NSWAN or does NATO seek dedicated on-prem solutions to a NATO/DoD data center?	6.At this moment, no commercial cloud provider infrastructure is available via NS-WAN. NATO needs to store the data in a dedicated on-prem solution.
7. Regarding 3.2 Capability, "Be a scalable system in order to get connected to other (national CCR) to host more user and/or to	7.The NCCR shall be extendable over time (new hardware and software), depending on the

provide more functionalities". Please elaborate on whether scalability is hardware and/or software, and enumerate the other range(s) with details on specific requirements.	technical developments and NATO's transformation over time. Some NATO Nations are running their own CCR's. If possible, these CCR's to the NCCR via a generic interface/standard.
8. Regarding 3.3 Capability, "Meet the requirements for the accreditation on a NATO classified network". Please detail the accreditation requirements.	8.The NCCR shall be accredited up to NATO SECRET. If this is not possible, it shall be mentioned which functionality prevents the accreditation.
9. Is there a current NATO Cyber Range solution in place? If yes, please describe.	9.NATO has no own/owned Cyber Range solution. NATO is using the unclassified Cyber Rang CR14 in Tallinn, Estonia.
10. Regarding 3.5 Capability, "Connect secure to other NATO entities". Please define the meaning of a NATO entity.	10.NATO entity is used as a generic term. In general, every NATO Nation, every NATO body (NATO HQ ESCD, CTAP, etc.), and every NATO Agency (NCIA, NSPA, etc.) shall be able to establish a secured connection to the NCCR.
11. Regarding 3.6 Capability, "Use data from the current exercise". Please provide more specificity on what is meant to "Use data" from the current "exercise".	11.The NCCR shall be able to collect data from on-going exercises and to use them for other exercises or for post-exercise assessments. The NCCR shall be able to import data from several exercises (Cyber Coalition, CMX, etc.).
12. Regarding 3.7 Capability, "Provide data for further deeper analysis". Please be more specific regarding the "data", what type of analysis will be performed on the data, and whether the data will be required to be exported from the platform.	12.The data will be needed to perform the post-exercise assessment. For this assessment data like log-files, behavioural data, etc. are needed. The data will also be needed to assess the behave of a digital twin and to assess if TTP or other processes are realistic and useful.
13. Regarding "Collect data and provide reports upon request". What is intended to be in these reports?	13.Reports are needed for the post-exercise assessment. Reports are also needed to assess the behave of tested tools, etc.
14. Regarding "Support an auditing functionality". What type of auditing is desired? Is auditing of the users engaged on the platform or in the range itself?	14.The NCCR shall support the auditing of the users of the platform. If an audit in the range itself is necessary, depends on the national laws of the host nation, which is not decided yet.
15. What localizations requirements exist for the proposed solution?	15.There is no specific geographic location for the users. For the use of the NCCR three different scenarios are possible. • Classroom right next to the NCCR, in a secure physical environment. • Users should be able to connect to the NCCR via an encrypted point-to-point connection • Users should be able to connect to the NCCR via NS-WAN (only if feasible)

16. Regarding 3.8 Capability, "Capability to create models based on roles definition". Please be more specific regarding this capability.	16.Depending on a rough description of an entity (system, enemy, etc.), the NCCR shall be able to create a model, which can be used in the NCCR/scenario.
17. In what location is the NATO CCR planned to be hosted?	17.Physically, the NCCR has to be in an NATO SECRET accredited facility. There is no decision for a geographic location, yet.
18. Are there any requirements for access to vendor source code?	18.This might be necessary for the accreditation process, but this question cannot be answered by ACT.
19. What is the scale of the planned NATO CCR? How many users? How many VMs? How many concurrent events?	19.The NCCR shall be scalable and expandable. Because of limited workforce resources within the Cyberspace Domain, concurrent events on the NCCR are unlikely. Number of users is depending on the exercise. Currently, NATO's biggest Cyberspace Exercise has roughly 1000 users.
20. Is the plan to include simulated Operational Technology (OT) within the NATO CCR?	20.This could be an additional/future scenario for the use of the NCCR.
21. CRA5-2 – please elaborate (The NCCR capability shall be able to connect to internal and external providers (within the accredited network (NSWAN))	21.Within NSWAN NATO has several internal data/information providers (like the intel community) the NCCR shall be able to be connected to these providers to exchange information. The same counts for external providers, like Nations.
22. CRA5-2.1- please elaborate (The NCCR capability shall be able to interface NATO's Cyber Situational Awareness capability)	22. NATO is developing a Cyber Situational Awareness tool. In order to get information from this tool there is a need for a generic interface/protocol, to integrate these information into scenarios.
23. CRA5-2.2 – please elaborate (The NCCR capability shall be connected to the NATO Cyberspace Security Center (NCSC))	23.In order to exchange information with the NCSC there is a need for a generic interface/protocol.
24. CRA5-2.3 – please elaborate (The NCCR capability shall be connected to the Cyber Operation Center (CyOC))	24.In order to exchange information with the CyOC there is a need for a generic interface/protocol.
25. CRA5-2.4 – please elaborate (The NCCR capability shall be able to exchange data with Intelligence sources)	25.In order to exchange information with other sources there is a need for a generic interface/protocol.
26. CRA5-3.1 - we don't understand what NATO means by 'framework' here.	26.Framework might be the wrong word. The NCCR shall be able to accept a pre-defined scenario as a starting point for further scenario development work.

27. CRA5-5.2 - what kind of data NATO wants to extract?	27.Log-files Behavioral data Snip-it's from scenarios
28. CRA5-5.4 - what kind of settings and how NATO wants to export them from CR?	28.Configuration files System files VM's Etc. These files/settings should be in a generic format. The export should be supported by tool.
29. CRA5-5.5 - what does NATO mean by 'models' here? What kind of 'roles'?	29. Depending on a rough description of an entity (system, enemy, etc.), the NCCR shall be able to create a model, which can be used in the NCCR/scenario.
30. CRA5-7.4 – please elaborate (The NCCR capability shall meet the requirements for the accreditation in a NATO classified network)	30. Because the NCCR will be/might be used within the NS-WAN environment, it has to be accredited for this environment.
31. CRA5-7.5 – please elaborate (The NCCR capability shall be operating with respect to confidentiality and integrity of data)	31.Confidentiality, no uncontrolled information/data outflow shall be possible. Integrity, no uncontrolled change/adjustment of data/information shall be possible.
32. What network classification levels integrations are expected?	32.Up to NATO SECRET
33. Any must-have certifications (resources/products/networks) are expected? Please specify.	33.This depends on the provided solution. Currently, there are no must have certification, except for the accreditation up to NATO SECRET.
34. Any product/solution/technology within the solution have any limitations that are allowed to be used? e.g. no open source or only open source, no VNC, no ruby etc.	34.As long as the product/solution/technology does not prevent the NCCR from accreditation, there are no limitations at this stage.
35. Where solution expected to be hosted and is there options?	35.Physically, the NCCR has to be in an NATO SECRET accredited facility. There is no decision for a geographic location, yet.
36. Connect to internal and external providers - what it meant under providers? Kind of software or networks?	36.Within NSWAN NATO has several internal data/information providers (like the intel community) the NCCR shall be able to be connected to these providers to exchange information. The same counts for external providers, like Nations.
37. Interface Cyber Situational Awareness capability - generally, what kind of capability expected? e.g. API control, exports, sync etc.	37.NATO is developing a Cyber Situational Awareness tool. In order to get information from this tool there is a need for a generic interface/protocol, to integrate these information into scenarios.
38. Which kind of data or type/issue/instance expected to be synced and imported/exported in the scope of NCCR activities for trainings/development/testing?	38.Basically, all data/information which can be used to revise, evaluate and assess the exercise should be synced and imported/exported. There is no comprehensive list, yet.

E.g. sources, scenarios, VM’s, data, flows, networks etc.	
39. Before committing to a full response to the ongoing RFI, I wanted to ask whether you are interested to hear about partial/peripheral capabilities? We can offer a well developed and tested tool for Situational Awareness, which could be used as a data source for the NCCR.	39.Even if your proposal is a great tool for Situational Awareness and might be able to provide data and information for our scenarios, it is too niche and out of scope for this specific RFI. However, ACT will issue another RFI with regards to Cyberspace Information Sharing and Situational Awareness really soon, and the tool might be the answer for this RFI. I encourage you to check our ACT Contracting portal https://act.nato.int/contracting where we publish our solicitations and RFIS