NECCDC 2022 | Info Session Q&A

Q: How are the NOC and SOC roles split? How would this new dynamic look? Would students be in the same room and would they only be able to touch certain systems?
A: We imagine around two members of the team (most likely) that would be focused on SOC tasks (not necessarily in a different room). They are envisioned to not be involved with O&M (operations & maintenance). SOC would not likely be doing injects, but looking at the environment, overall needs, and providing recommendations for the broader team for them to look into. Might see callbacks within the environment or things of that nature.

Q: How many competitors will be allowed on each team?
A: See Nationals competitor rules 1&2 for more details on competitor eligibility and team composition: http://www.nationalccdc.org/index.php/competition/competitors/rules

Q: Will both Quals and Regionals be in person?
A: Quals will have teams at their educational institution, and Regional will be at Champlain in VT.

Q: What resources teams will get access to once they have registered as a part of the NECCDL (Northeast Collegiate Cyber Defense League)?
A: If you are a paid team, you would get the VM-50 Palo Alto and anything else we can give you with regards to resources. Also, the team packet will be provided when available / when you register and access to orientation and potentially other resources, e.g., Palo Alto training. To sum up: The sooner teams register & pay, the better.

Q: Can we use github?
A: Yes, for those who have played before, similar for this year there should be repos that are publicly available where it will be approved and shared with all teams. There is a specific timeline for when the items should be frozen (not changed). We are currently determining this date. See Nationals competitor rules 5 (and 5f specifically re: Scripts, executables, tools, and programs) for more details on “Internet Usage” and resource use during the competition: http://www.nationalccdc.org/index.php/competition/competitors/rules

Q: Will we get access to these slides / Q&A after the meeting to reference it later?
A: Yes, they will be available on the NECCDL website.

Q: Would it be possible to gain additional access to other resources (the more the better)? Some schools don’t have as much access to resources as others.
A: Depending on the scope, there might be some potential to help with providing resources across schools through NECCDL.

Q: Would there be limitations for those placed in the SOC role, or would those in this role be elected by members or specifically chosen by the competition. What types of responsibilities are expected of the SOC role / what tasks will they need to prepare for?

A: Teams would determine who would be placed in SOC / NOC roles. SOC needs to have mission data, e.g., event viewer / syslog as well as threat intelligence coming from the network. Looking to shift these tasks from the general blue team to a few members to ensure this information is getting reviewed and operations teams will be able to patch things and detect / block red team activity in the environment.

Q: How will threat hunting be taken care of? Will some tools be already prepared / fully functional or will they have to be installed?
A: Two boxes will be prepared (will be communicated through the Qual Team Packet in advance). The SOC hosts will have the tools already installed to use (will not need building, unless additional tools are desired).

Q: What are the communication methods to be used during Quals and Regionals for both NOC and SOC teams? Will there be a ticketing system or chatting in each room?
A: Communication flows are being worked out and we want to avoid unorganized communication. We're actively looking through a ticketing system for the teams for those communication flows. We also imagine that the SOC and NOC will funnel communications through team captain. We expect there to be penalties for breach of those communication restrictions, e.g., screaming = disorderly conduct.

Q: Would communication channels be in scope for the red team?
A: Communication channels would be official channels, and would be out of scope for the red team.

Q: Would a key individual be responsible for passing things between NOC and SOC teams - would you intend for each NOC and SOC team to have a leader designated?
A: Blue teams can choose to designate a leader for each NOC and SOC team, however, this will not be mandated. It would probably be beneficial for teams to do so based on overall team dynamic.

Q: If a team is not authorized to travel in Spring due to its University regulations, are there options for remote participation?
A: At this point, we envision Regionals to be completely in-person or completely remote for Regionals competitors. Unfortunately, if the competition is determined to be in-person, we will not be likely to have a hybrid experience with some remote and some in-person teams.

Q: What services will be scored?
A: Several of the services that were scored in previous years will appear this year as well, however, there should be expectations that some services may be novel this year.