

# NECCDC 2025 Season Info Session Q&A

Hosting Organization: Roger Williams University, Rhode Island

Friday Jan 3, 2025 at 6pm EST

Q: Curious if we would get some licenses from Palo Alto for practicing?

A: [Palo Alto Networks Academy](#) allows you to request licenses. Andrew I will look into potentially getting access. <https://mirror.cloudpropeller.com/paloalto/vm-series/>

Q: Are there other network devices other than the palos? Are we going to be using Linux bridges for vlans?

A: For qualifiers, not likely. Shouldn't have to touch interfaces in Qualls.

Q: Where can we submit moderator information?

A: The mod contact form will be included in the resources provided after this presentation!

Q: Since Splunk is a sponsor does that mean that Splunk will be used?

A: As of now, not yet.

Q: Any info on what backend/hypervisor will be used to run our VMs for quals?\* Will we have access to the VMs to Power on/off if needed

A: It will be on AWS and console access is not provided to teams (No)

Q: Any rationale for moving to Graylog vs. sticking with Wazuh

A: Not being used as a replacement. (You've seen it too many times)

Q: You said we are getting our internal network with a public firewall - what is the role of the empty public subnet box on the topology?

A: Look at the network diagram and draw your own conclusions. Go to the beta and you will find out.

Q: Will pipeline be Jenkins again or did the diagram say?

A: We can confirm that there will not be a CI/CD Pipeline. (Check the packet / slides)

Q: Will the scoring engine be available during the beta test? A great opportunity for Black team to test at scale?

A: Good chance it will be running. Most of the issues have been discussed and remedied. Blue team access is about 60%+ chance - probably will be a watered down version.

Q: Great to see Cobalt Strike back. To what degree will Red Team leverage Cobalt Strike this season?

A: Cobalt Strike never really left. If used in an environment, it will be used by Red Team.

Q: Can we utilize Palo Alto fw zones for segmentation? As it usually has to be allowed in the AWS backend?

A: Yes

Q: Is there any information on the version number that we will see? What major (and minor) version of PAN OS?

A: It will be a newer version (11.x)

Q: What is the best way to do backups for snapshots?

A: Look at the network diagram and the services to draw conclusions from that.

Q: It was said that the inject scoring system needs to always have access through the firewall - Are injects not submitted and scored through Google Classroom?

A: That was misspoken: injects should be submitted through Google Classroom, but do not block the SERVICES scoring service.

Q: Any suggestions on preparing for supporting "Open Source EMR" included in v1 of quals packet?

A: Look at the different OSS solutions [available](#) and draw your own conclusions. The name is very descriptive for what it is.

Q: What are "Living off the land binaries (LOLBINS)"?

A: Using tools that exist in an improper way to get access. There is a github repo or Fullstack that has access. <https://gtfobins.github.io/>

Q: Why is "PowerPoint" in the pack list?

A: All software is in scope.

## Friday Oct 11, 2024 at 6pm EST

General Black Team Advice:

Work on the fundamentals. Have people work on specific processes, operating systems, or just down to setting up a SIEM and make sure that people are familiar and comfortable moving around. Try to practice on [infrastructure](#) you saw in previous years.

---

Q: What if we are excited about the HackTheBox CTF?

A: If interested, please reach out to Chandler Anderson. Reach out to him or Joe E (NECCDL). Will have a higher edu CTF in December as well. [Chandler@hackthebox.com](mailto:Chandler@hackthebox.com)

Q: For HackTheBox what format is it?

A: It is Jeopardy style and will be a 24-hour event. 1 team per college/university. Market to coaches. Will have multiple different options. It will be 6:00 pm Eastern. (Challenges have been tuned towards Blue Teams)

Q: What training resources will be available?

A: Palo Alto training will be available (probably feed into Regionals). Will have a more in-depth network diagram in early December. Will have a high-level understanding of the infrastructure. Will have information about training when we release high-level infrastructure via the packet.

Q: Is there any appetite for something in-between - like a scrimmage?

A: Yes, if that can be supported, we will try to make it work. Joe A would also be willing to help facilitate. CCDC-esque, but not necessarily NECCDC, but helps with preparation.

Q: Will the slidedeck be released after today?

A: Yes, we will post it on the website and also the Q&A.

Q: What should you incorporate into training?

A: Automation, scripting is important. Often see blue teams doing tasks manually which takes a lot of time that could be used elsewhere. Focus on getting the basics under your belt first. (KISS)

Q: Competitions were used as a great way of proving outcomes of the NICE framework and AI-related NSA CAE KSA's.

A: For applying competencies in real-world scenarios helps enforce that level of competency. There's nothing like it to incorporate hands-on learning.

Q: Will the first packet be released at the next meeting in December?

A: We will release more infrastructure at least by then.

Q: Will CCDC Nationals be virtual this year? Can it be confirmed or denied? What can we do?

A: Yes. Official announcement will be out next week. Nationals will be virtual. Raytheon, an RTX company, will no longer be the large National partner / sponsor. If you're willing to help out and suggest sponsors for NECCDC please let us know. We have OCEAN regional educational network (REN) which serves every higher edu, health-care provider and had a call early this week. Excited to be a sponsor this year and will help make contacts with healthcare institutions. Hoping to increase sponsorship this year. A lot of fundraising before qual.

Q: With the high level architecture slide, does the Erlenmeyer Flask icon represent some scientific equipment webui?

A: Yes (see the list of infra bullet points, can hint to what it might be)

Q: My team competed in a MWCCDC invitational competition last November that really was helpful in gaining practical skills about how to compete and get to know the process. I'm unsure if they're doing it again.

A: Yes, it's a great opportunity. No, we have not heard anything about either.

Q: Is HM Linux Hannah Montana Linux? <https://hannahmontana.sourceforge.net/>

A: Yes.

Q: Would be interested in seeing new team sponsorships in regards to funding. It was helpful last year, and would like to see more of that.

A: #1 priority is to make sure that the hosting institution is covered, and then it will be a consideration.

Q: Have alumni at undersea warfare center, while may not be able to get sponsorship, can get volunteers - Ben Grooms.

A: Anyone with alums to recommend contacting, please also let us know.

Q: Do the colors of the backgrounds on the Windows and Linux boxes on HLA signify server/workstations or am I reading too deep?

A: No comment. :)

Q: How can you get more spoilers?

A: Will be putting out teasers through the platforms, which would be helpful to monitor.

Q: When is the repository freeze date?

A: Same date as registration deadline in January. (Archive your repo)

Q: Is Wazuh still in play this year?

A: No comment.

Q: If there's no macOS in the HLA diagram, but it's mentioned off to the side, will macOS be out of scope or it just didn't make the cut for the diagram?

A: Could be there for Regional or Qual. Not decided yet. This will be confirmed in future packets. Think about general categories of what you saw in a high-level overview diagram.

Q: Is there an open-source EMR platform?

A: No comment (see diagram).

Q: Assume running EMR off of OCI?

A: OCI has multiple acronyms.

Q: Will AWS be in play?

A: It has not been confirmed, see the high level infrastructure diagram.