NECCDC 2024 | FAQ

Regional Orientation | Q&A - Friday Feb 23, 2024, 6pm ET

Q: For the “individual” who is getting the hotel reimbursement, can that individual be the University? How would it work if my university fronts the cash for hotels / travel, would Pace reimburse my university?
A: Yes - will follow with an email with details.

Q: Are two nights allowed? What about parking reimbursement?
A: The plan is to reimburse up to $1,500 for hotel expenses. Since hotel spending is typically the biggest bill, we plan to do that. The reimbursement is based on travel receipts.

**Rooms booked any of 3 nights count as part of the $1500: 3/22-3/24
**Parking is not reimbursed

Q: ETA for Regionals packets
A: Ideally this weekend and this upcoming Tuesday at the latest.

Q: Will we have admin access on the laptops?
A: Yes (No, root access)

Q: To what level is Cisco in scope?
A: The Cisco devices (Meraki switches) are in-room for purposes of getting everyone on LAN to get VPN tunnels established. **Out-of-scope for everyone** (blue and red teams). Cisco switch will be a dumb switch.

Q: Is AWS in scope?
A: AWS console access will be in scope. Access controls, networking and instances in AWS will be available to blue teams (similar to last season).

Q: Are we allowed to bring any peripherals? (Mice, keyboards, monitors, headphones, etc.)
A: Yes, monitors are special accommodations. Will need to be approved prior to competition - can send ahead of time via blackteam@neccdl.org. Notify us ASAP if you need a monitor for accommodation. Information will be added to the Regional packet.

Q: Will monitors be provided?
A: Each team will be provided two monitors. Work it out with the team who needs it the most.

Q: What is the role of coaches while the team is competing?
A: Not doing any interaction with teams. In a coaches room, mingling with other coaches. Maybe seeing NYC. Should be within close distance of competition.

Q: What sorts of things are we going to be allowed to do in AWS besides implementing network controls? ex. taking EC2 snapshots? What AWS services beyond EC2? IAM, S3, CloudTrail?
A: Everything is testable within the free tier. AWS services are generally available on all cloud platforms.

Q: Should we expect the Red Team to attempt physical access into blue team rooms this year? Will Red Teams be able to break into Blue Team rooms?
A: One pace plaza is a pretty modern building. Have classrooms that will have auto-locking doors with swipe card access. Day of competition will have rooms open and unlocked but will start to auto-lock after a certain point. After competition closes, theoretically can't get in unless a card gets them in or door kicked in. Each team has their own room.

Q: Do USBs need to stay in room overnight btw comp days (and are they in scope for RT?)
A: USBs (and any equipment provided by competition) needs to stay in the competition rooms as it is not supposed to leave the competition environment.

Q: Are the Red Team able to try to get in during hours?
A: They can ask to come in. There will be ways to respond in case there. You are always free to ask someone to leave politely. If they do not leave, make sure to let your moderators know to report. Keep in mind there may be some legitimate in-person orange team events that need to be addressed and will impact scoring.

Q: Can we bring a projector that fits in a backpack?
A: Send it in for pre-approval of peripherals.

Q: Are we allowed to shift services to another OS/platform during competition?
A: May cause more trouble to try and switch vs. patching and making sure it's protected.

Q: Will team captains have access to the environment?
A: All team members will have similar access.

Q: Could coaches get tours of the ECE facilities?
A: In general, not a problem. Can go to a robotics lab. Will also be looking at Computer Science facilities. The cyber range is at the Pleasantville campus so it is likely that there will be no time to tour that facility.

Q: What's the role of the PLC looking like for regionals? (I was told during the quals info session that it was going to play a "larger role")
A: In Qualifier, they didn't really have a functional role. It will be utilizing its logic in Regional. Have an environment simulating (hydroelectric dam scenario) so have components in scenario, dam with water level, spill gates, water flow and turbines. PLC's job is to control and execute logic on the environment. The simulation is out-of-scope and intelligent electronic device that gives ground truth visualization is also out-of-scope. PLC and HMI are in-scope for competition. Blue teams should protect them. PLC will have some interaction with other things outside of the OT environment (IT env, business applications, generating electricity, distributing electricity and trading for energy and electricity). Boundaries between those distinct parts of the network and part of protection - being aware of what is on network segments, etc.

Q: Can we use the projectors in the room?
A: No, those constitute the A/V equipment that has a specific purpose.

Q: Will there be more use of IdM for regionals? if teams want access to RHEL repositories do they get access to that too? (didn't get access during quals).
A: You can use the fast-tracked version of the software FreeIPA which can be installed fairly easily on RHEL (Red Hat development plan - free with school email) or Fedora. IdM will be in Regional's access and will remain the same as Qualifier (ui & access).

Q: Is network topology the same as in Qualifier?
A: No.

Q: How much deviation from Qualifier topo?
A: There will be updates in the Regional packet.

Q: So do we have unlimited EC2 access? As in can we make new ones?
A: Not unlimited. Unless you want to share your banking info. 😉

Q: CrowdStike is a sponsor: Will CrowdStrike Falcon or other products be available for use?
A: No. We can try to ask the sponsor if it would be able to be used for the competition.

Q: Does Pace provide any bus transportation from metro hubs?
A: No, the subway station (Brooklyn Bridge) has a 50’ ft distance from entrance to One Pace Plaza.

Q: We have team members on our roster that require a medical device to be on their person to administer medication on a scheduled basis, will they be allowed to have their phone close by in the competition to monitor their health and the device?
A: We’ll discuss med tech devices in the Regional packet. 100% if it is a medical requirement, we want everyone to stay healthy for the event. Please just follow up with a formal request in accordance with Regional Packet once released

Q: In our team's feedback, we were told to expand more on business impact for our reports, and this is something I'm sure lots of teams have struggled with. Could you give a valid example of business impact in an incident response report?
A: Here’s a blog post from a Red Team member, discussing IR reports. Also, National CCDC Rules provide some guidance on IR reports as well (9.d).

Q: Please explain what an intel [intelligent] electronic device does (in the real world, and potentially its function for the comp).
A: Industrial control system lingo for components in that space. Hardware interface or for OT people. What we wanted to do was put them into Blue Team rooms to see ground truth. Imagine things will go wrong on the OT network side or the HMI which impacts the environment + damage will show up somewhere. One of the purposes is to show if it goes “red”, then there is a critical problem endangering human life.

Q: Was the logo created with gen AI?
A: Yes, it was. The bottom wasn't there since the letters were in all the right places. :)

Q: Will we get a reimbursement if we don't fill out the NSF grant form?
A: No. :) Please fill out the form emailed earlier for the NSF grant report, or ask for a re-send.

Q: Will there be Pace security for check-in?
A: There will be a list of people who are coming in and there will be verified. Will need to get everyone's name, email & phone number. Also, expect a photo release form.

Q: Is there a need to be proof of COVID immunization still?
A: See: https://www.pace.edu/student-accounts/immunization-compliance/immunization-compliance-requirements The COVID-19 vaccine mandate will no longer be in effect, and proof of vaccination will no longer need to be submitted for students and employees.

Q: Does the hotel having contracted have decent parking for at least one vehicle?
A: Nothing with parking and no affiliation. Lot a block away. See what they have. Can use google maps provided by NECCDC 2024 with at least four different parking lots.

Q: Can there be a Regional coaches and separate memes channel? Will there only be team captains in the team channel?
A: Yes.

Q: Ever thought of using Discord Stages?
A: Did consider doing 2021, but had a cap at that time. Can re-evaluate as an option this season.

Info Session #2 | Q&A - Thursday Jan 4, 2024, 6pm ET

Q: What's the URL for Authorized Repo's?
A: Authorized Repos | NECCDC 2024

Q: What's the PDF for RT Advice?
A: Advice_from_NECCDC_RT.pdf

Q: Do you have advice for how teams should discuss root cause when RT malware/tools were built into the systems prior to the competition?
A: The reason why RT puts things on systems ahead of the competition is to be fair. Those that don't pre-deploy is a problem in that only 9/10 teams are affected due to the timing so that team

gets a free pass with no implants. Most malware tools have a persistence system (if you can find and get rid of it / or reboot and have it go away … then do that). This happens at Nationals more, and we bring this to Regional (one or more systems vulnerable to end-day. Need to be able to identify systems and fix vulnerabilities, or block attackers.

Q: Will https://neccdl.org/neccdl/members/ be updated by the 20th?
A: Yes, the website will be updated as soon as possible. We do have a lag receiving information from Nationals.

Q: Do teams need to compete together in the same room and/or on-campus for the beta?
A: For the beta, the teams don't need to be on campus or in the same room, but yes, it is highly recommended as it helps with practice. However, we realize that it's not always possible for some teams based on break times.

Q: Do you want any cameras on during the qualifier?
A: For authentication purposes, team members bring a valid school ID which on-site moderators validate.

Q: Will there be another window for Github submissions before Regionals?
A: Unfortunately, there is not another window for Github submissions before Regionals due to Nationals rules.

Q: Are we still using ScoreStack, another open source project, or Nationals scoring engine?
A: We are using ScoreStack.

Q: If we are a first time team (i.e. still trying to finalize a faculty sponsor) and end up registering/submitting roster on Jan. 19, do we still need to submit a moderator on that day?
A: We can generally help with new teams. Also, you just need someone affiliated with your institution to be the coach, e.g., IT staff, prof, etc.

Q: Is there a suggested hotel, or a hotel that Pace is working with for the regional?
A: Waiting for a response, but for now, https://www.pace.edu/nearby-hotels
Millennium Downtown Hotel World Trade Center 55 Church Street New York, NY. 10007 (212) 693-2001 Exclusive discount offer for Pace University affiliates: 20% off the best available rates. Also Holiday Inn Financial District 51 Nassau Street New York, NY 10038 Exclusive discount offer for Pace University affiliates: 15% off the best available rates (Financial District location only). Use Corporate ID # 100203474 when booking. Book online or call (855) 914-1383 for reservations.

Q: Are there any scholarships or grants for participation in Regionals?
A: We will see what the numbers look like. If you are aware of any potential sponsors, please do connect us to sponsor@neccdl.org

Q: Are there updates on parking?
A: Waiting on response - will get sometime next week

Q: 3 windows servers, only AD shown in service list? Is CA no longer a service? Or file stuff?
A: AD consists of a lot of moving parts. You will see the typical parts in play domain services, DNS, and will probably see a CA somewhere since you need an element of trust in the environment. Need to trust yourself, teammates, and ensure your machines can trust each other.

Q: Wireguard is not in new topo, will blue teams use a different access method?
Is CA handled by Vault?
A: Wireguard will be the main entry point for blue teams. Can't currently answer Vault question.

Q: It was stated that there won't be much of the "competition theme" during Qual, but the diagram we were shown during the session features a PLC. Does this mean we should expect to see some level of OT during quals?
A: What we mean is not a lot of injects related to OT stuff. This is a cyber defense competition, and not PLC management competition. Wanted to add an element of ticking services you need to keep running like your other ones, that we can relate to the OT side of things. In no way will you be asked to be OT operators. However, you are the Blue Team who has governance over the complete IT + OT infrastructure. Having responsibility for what happens on that OT network will be yours. Having an awareness of asset inventory on OT and the boundary of IT/OT will be yours. In Qual, PLC will exist and may be a component of scoring, but won't have any functionality besides being there. Won't have functional dependencies or dynamic things going on in that space. For Regional, this will change.

Info Session #1 | Q&A - Friday Oct 20, 2023, 6pm ET

General Black Team Advice: Emphasis on RHEL IDM/FreeIPA, look into automation. For Qualifiers no AWS console access. Will be new technology that you have to learn that will be foreign to you. Credential management and Kubernetes. Some subject to change. Some would be taken out, not put in.

Q: Will the presentation be made available to share?
A: Presentation and Q&A documents will be shared after review for accuracy

Q: Do you have an anticipated time frame for knowing about hotels?
A: Have an idea of what hotels will give a discount rate. Can probably get out within a few days.Will keep trying to get better rates, but have a short list.

Q: What are the discounted hotel rates looking like?
A: https://www.pace.edu/nearby-hotels - discounts up to 20%

Q: Travel?
A: Consider travel - parking is not readily available.

Q: For firewalls - there was Palo Alto, training, is there more insight?
A: With host-based firewall rules, lots of iptables, Windows firewall, and other OS that show up. Can provide documentation that will give insight. Want to make sure you're comfortable with services. Talked about virtualized appliances in quals, but believed may be pushing too much. Host-based firewall rules would give a good foundation for a mindset for more centralized management.

Q: Qualifier / Regional Remote
A: Will be remote in that not all teams will be in the same location physically. However, all teams are expected to be physically present together on their campus in the same location. If there is a need for an exception, it needs to be discussed between the Coach/Edu Rep, the Director, and NECCDL.

Q: Is there a time when we should have moderator contact information?
A: Will be near the registration deadline. Please recruit people who have some experience, e.g., alumni, industry, or local professional organizations. Let us know if you are a new team and/or you need help with moderators.

Q: Will AWS resources be provided for blue team prep?
A: Learning materials can have links provided. The free tier for AWS - focus on VPC and Security groups.

Q: What should you advise for AWS setup?
A: AWS offers free training through AWS Academy. Can use the free tier for configurations for security groups, how to backup an instance, take a snapshot and if you can run things on your local hypervisor, go for that. Learn services on own infra and then learn AWS via AWS: https://aws.amazon.com/education/awseducate/

Q: The line between Qualifier and Regional?
A: In Qual, will not have AWS console access. Emphasis on host-based firewalls there. Andrew can recommend some labs that AWS Educate provides.

Q: MacOS?
A: AWS does provide MacOS AMI's for virtualization for EC2 instances. Up in the air right now with Black Team in discussing implementing that concept. Not a critical role, but in a typical world, you will see Windows and Mac. Definitely train for it. 99% will see in Quals or Regionals.

Difference between AWS and hypervisor, if you were to allocate money to AWS, spin up some MacOS EC2 and play for an hour or two. Wouldn't spend too much time on it, but should know how to do the basics with it.

Q: WIll the Regionals be held in Manhattan or Westchester?
A: Manhattan

Q: What about safety concerns?
A: Can get a meeting with the emergency response / security department. The campus location is a pretty safe area and students frequently take a train down there. Can get a more outlined approach for security. Don't have the information at hand now.

Q: RHEL 8 or RHEL 9?
A: Hint: Version listed in AWS AMIs