HOSTED BY

Roger Williams UNIVERSITY

IN COORDINATION WITH

PRESENTS THE

NORTHEAST COLLEGIATE CYBER DEFENSE COMPETITION

2025 SEASON QUALIFIER

BLUE TEAM PACKET

1.3.0 | 2025-01-24

CONTENTS

NORTHEAST COLLEGIATE CYBER DEFENSE LEAGUE

The Northeast Collegiate Cyber Defense League (NECCDL) is an administrative body whose sole purpose is to facilitate the smooth running of NECCDC regardless of hosting institution. The League is operated by academic volunteers and is funded by league sponsors and annual membership fees collected from participating Academic Institutions.

Find out more at: neccdl.org
LinkedIn: northeast-collegiate-cyber-defense-league
GitHub: github.com/NE-Collegiate-Cyber-Defense-League
Follow on Mastodon: @neccdl@infosec.exchange
Follow on BlueSky:@neccdl.bsky.social

We would like to thank Roger Williams University for hosting the qualification infrastructure for this season!

NECCDC 2025 SEASON

The Northeast Collegiate Cyber Defense Competition (NECCDC) is designed to provide a controlled competitive environment that will permit each participating institution to assess their students' depth of understanding and operational competency in managing the challenges inherent in protecting enterprise network infrastructure and business information systems. NECCDC provides an opportunity for qualified educational institutions in the Northeast to compete in this environment and is part of a national organization (nationalccdc.org), which provides a unified approach for nine regions across the country. Qualified educational institutions include those with information assurance or computer security curricula.

Competition Goals

1. To promote fair and equitable standards for cyber defense and technology-based competitions that can be recognized by industry
2. To evaluate the defensive and responsive skills of each team under hardware, software application, and operating system configurations using a joint academic and industry rating scale
3. To demonstrate the effectiveness of each participating institution's academic security (and related) programs
4. To be executed by a preponderance of industry professionals
5. To have industry recognition, participation, and acceptance of each competition

6. To rate the effectiveness of each competition against a predefined standard of competition rules
7. To provide a cooperative and competitive atmosphere among industry partners and academia in the area of cyber defense education
8. To provide recognition for participating teams
9. To increase public awareness of academic and industry efforts in the area of cyber defense education
10. To facilitate the pipeline for the next-generation cybersecurity workforce
11. Develop competitor skills to respond to modern cybersecurity threats

Qualifiers Overview

The NECCDC 2025 Qualifier is managed by this year's competition host (Roger Williams University), with strong contributions from the wider team at NECCDL with representation from various academic institutions and industry organizations. The competition is designed to test each competing team's ability to secure a networked computer system while maintaining standard business functionality.

In the healthcare sector, third-party risk management is critical to safeguarding sensitive patient data and ensuring regulatory compliance. As healthcare organizations increasingly rely on external vendors for services like cloud storage, billing, and IT support, they face heightened risks from cyber attacks, data breaches, and operational disruptions. Effective third-party risk management involves assessing vendors' security practices, implementing robust contract management, and conducting continuous monitoring to mitigate potential vulnerabilities. By proactively managing these risks, healthcare providers can protect patient privacy, maintain trust, and adhere to strict regulatory frameworks like HIPAA and HITECH.

The competition involves more than the application of technical skills. It is also one built upon the foundation of business operations, policy, and procedures. A technical success that adversely impacts business operations will result in a lower score, as will a business success that results in security weaknesses.

Qualifying teams from the **NECCDC 2025 Qualifier on February 1, 2025** will have the opportunity to participate in the **NECCDC 2025 Regional**, expected to take place **March 14 - 16, 2025 at Roger Williams University** (1 Old Ferry Road, Bristol Rhode Island) - the host organization for 2025.

NECCDC 2025 Season Sponsors

NECCDC would not be possible without the generous support of our sponsors!

Additional information regarding sponsorships for the NECCDC 2025 Season can be found at neccdl.org/sponsor and neccdl.org/history/2025.

GOLD
National Security Agency – United States of America

SILVER
Cisco Networking Academy
paloalto NETWORKS
splunk> a CISCO company

BRONZE
FORTRA Cobalt Strike

OTHERS? HELP CONNECT US WITH POTENTIAL SPONSORS!
Others TBD, in contracting. **Let us know if you have someone you know who is interested in sponsoring!** **Have them contact sponsor@neccdl.org for more information.**

QUALIFIER BETA SCHEDULE (*optional*)

- Qualifier Beta Test: (optional, but **HIGHLY** recommended) this is a small test run with no points in play, with access to a portion of the game environment allowing reconnaissance and/or planning.

Saturday, 25 January, 2025

TIME (EST, 24-Hour format)	ACTIVITY
09:30	Stock up on snacks and drinks in close vicinity
10:00	Opens mock game infra access
11:00-ish	Expect Test Inject within Google Classroom
12:00	Close mock game infra access

QUALIFIER EVENT SCHEDULE

- Please be in Discord and On-Site at your educational institution-provided space ~20 minutes prior to Check-in time.
- Have a webcam/video capacity + Student ID for authentication.
- Work with your Team's Moderator(s) (and be prepared to feed them!) - if your coach hasn't already, & make sure they submit moderator contact information for training and coordination.

Saturday, 01 February, 2025

TIME (EST, 24-Hour format)	ACTIVITY	NOTES
09:00	Blue Team Check-in Begins in Discord / Should be on on-site location at your educational institution	Have student ID accessible
09:30	Welcome Inject	Injects in Google Classroom
10:00	Competition Begins	Scoring starts and Blue Team access to environment systems enabled. Credentials are shared in Discord.
14:30	Competition Ends	Blue Team access to environment systems will be disabled.

Competition Organization

Blue Team

Student team representing a specific academic institution or major campus competing in the NECCDC. Each team must submit a roster of up to 12 competitors to National CCDC via: https://www.nationalccdc.org/index.php/competition/competitors/registration (due by Jan 24, 2025). Each competition team may consist of up to eight (8) members chosen from the submitted roster. The remainder of the roster is for substitution in the event a member of the active competition team cannot compete. Substitution in the competition team requires approval from the Competition Director.

- Students should maintain a full-time status (as defined by the participating institution) at the time the competition is conducted. Coaches are responsible for ensuring that participating students have the status needed to participate, and recommend two (2) or more moderators. See National CCDC rules for full eligibility criteria.
- If there are **technical issues** use the **@BlackTeam** handle in your team specific Discord channel for infrastructure-related questions. If competitors are unsure about **other questions**, then they should ask their room moderators.

White Team

Representatives who serve as competition officials, moderators and rule enforcement in the various competition rooms. You can use the **@WhiteTeam** handle in your team channel for any inject-specific questions that are not sent through moderators.

- Each team competing remotely from their home institutions must have at least one (1), ideally two (2) or more, site moderator(s) present at the blue team location as well as within the virtual environment during active times of the competition provided by the Team Representative.
- Moderators are responsible to perform tasks such as:
    - Undertake/Review moderator training offered by NECCDC
    - Gain familiarity on using the required communication tools (e.g. Discord)
    - Submit questions/requests from the blue team members to the designated communication channels
    - Check rosters to authenticate competitors at check-in
    - Ensure that competition rules are followed and any violations or situations of concern are reported to the White Team senior staff
    - Submit survey feedback based on competition/team observations near the end of Qualifier (e.g., webform provided in Discord)
- White Team senior staff will:
    - Supply and score Blue Team tasks in the form of competition injects
    - Adjudicate the scoring for the competition
    - Have a chief judge responsible for final decisions with regard to scoring

Black Team

Competition technicians, the Black Team develops, deploys, and maintains the competition environments. It also configures remote access, Discord, the service scoring engine-related, and helps write technical injects alongside the White Team.

Red Team

Professional network penetration testers from the industry, approved by the Competition Director, and industry representatives who:

- Scan and map the network of each competition team - Attempt to penetrate the defensive capabilities of each Blue Team network
- Modify any acquired environment
- Assess the security of Blue Team networks
- Attempt to capture and/or modify specific files on targeted devices of Blue Team networks
- Attempt to leave specific files on targeted devices of each Blue Team network
- Document and provide feedback for competitors/organizers to evaluate performance
- Follow Rules of Engagement for the competition

Gold Team

The competition staff includes the Director, logistics, and sponsor relations coordinators.

Orange Team

The competition staff builds an integrated scenario storyline and simulates user activities in a manner that integrates with and contextualizes Black and White team activities. The team also may include individuals who act as employees, clients, and other external acting parties, e.g., C-suite personnel, law enforcement agents, etc. These actors may interact with infrastructure systems and the Blue Team members during the competition experience.

Competition Rules

NECCDC subscribes to the National CCDC Rules, which have been continuously updated in recent years. In particular, Article 7 on Professional Conduct which applies to competitors and non-competitors alike. Not only is this expected in today's workforce, we truly strive to create a fun and safe professional + technical learning environment every year.

The Director will update a list of published Blue Team GitHub links for Qualifier. Besides these approved repositories, teams are **not** allowed to use **any private** staging materials. Please publicly archive your repository during the freeze period.

Competitor Authentication

Competitors will be expected to show a valid/current student ID, issued by their educational institution to authenticate during the qualifier check-in. Authentication will be done by room moderators on-site at your educational institution.

Blue team members should ask for rule clarifications through their room moderators at any time. Scenario-based activities can take a wide variety of paths, so if there is any doubt or need for clarification on injects or other competition-related events, make sure to check with room moderators who can relay questions to appropriate competition staff.

Questions and Answers

We maintain a set of Questions and Answers from our information sessions, publicly available here: FAQ. As teams onboard, updated communications will be in Discord.

Scoring Overview

Blue Teams gain points throughout the competition in two (2) categories using the following point distribution:

50%	System Scoring
50%	Inject Scoring

Both service uptime and completion of injects are equally important. As with any business, systems often have different risks and criticality. Additionally, any disabling/disconnection of network services is considered unauthorized and thus, depending on severity and service criticality, might incur appropriate SLA violations. The more points Blue Teams can gain, the better.

Additionally, successful Red Team Activity will subtract up to 50% of points from a team's possible total points:

- 50%	Red Team Activity

The more points Blue Teams can prevent the Red Team from taking away, the better.

Accurate and high-quality Incident Reports will reduce the number of points reduced as a result of Red Team activity.

System Scoring

System availability and integrity make up half of the Blue Team's final score. This scoring consists of service checks that happen on a predetermined interval. Each successful check will increase point totals (depending on service criticality). Unsuccessful checks will not add or decrease point totals.

Points can additionally be lost from failed employee access (described later in this section) or by requesting Black Team intervention on your systems (See 2025 season - Black Team Operational Aid Charges).

Inject Scoring

Injects are business tasks provided to each team throughout the competition and make up half of the Blue Team's final score. Injects are typically provided to teams in the form of communication from a supervisor/stakeholder, a project work order, or a break/fix ticket. Injects may not always explicitly outline specific deliverables expected. It is the responsibility of the Blue Team to interpret the request and respond professionally. Questions can be asked for clarification via moderators or directly to White Team or Black Team. Some injects may be scored objectively, while other injects may be scored on a ranked scoring model. Injects may not all have the same point value, and are weighted based on items such as complexity and time required to complete. The specific point value for each inject is not disclosed to the Blue Team. Injects have their own deadlines, and injects submitted past deadlines do not earn points. Keep in mind that the Google Classroom clock may be different from your system time and can experience lag when submitting.

Red Team Activity

Successful Red Team activity is subtracted from Blue Team total points. Red Team Activity has a ceiling and may not take away more than half of the total possible points from the combined service and inject scores. Accurate, evidence-based, and professional Incident Reports submitted by the Blue Team may provide the opportunity to reclaim Red Team points for specific Red Team activity. However, very low-quality Incident Reports may result in additional points awarded towards Red Team Activity and Blue Teams should only submit Incident Reports they have confidence in (detailed in National's Rule 9.d). A standardized Incident Report document is provided below and teams are encouraged to utilize the document to submit Incident Reports.

Incident Response Template

Please feel free to use this Incident Response Template, or use a similar professional IR report which captures data referenced in National Rules 9.d.

Tips for Effective IR Reports:

- Submit IR reports when incidents occur in order to potentially reduce future Red Team impacts.
- Ensure any executive summaries and business impact analyses are appropriately written for the intended audience (try not to include too much technical jargon).
- When writing, ensure that it is professional and includes enough necessary information and depth while not including any extraneous information.
- When discussing business impact, ensure that you accurately identify the effects on the business.
- Once an incident has occurred, you want to perform remediation. Any actions taken towards remediation/prevention should be detailed.
- Make sure that you include relevant screenshots, visuals & evidence.
- Think about whether what you are experiencing is really due to Red Team activity or due to a misconfiguration/actions taken by the team.

PlaceboPharma Employee Job Functions

While Blue teams must secure their environments against threats, employees must still be able to access systems to perform their jobs to keep the business functions operational.

During the competition, employee's access will be checked to ensure they can still perform their job functions. Access checks of a single employee on a single system will be performed every **30 minutes** after the competition begins.

If the employee cannot connect to the system, then the team will receive a warning in Discord. The message will contain the user and system that they are trying to access.

During the next 30-minute check, the previously failed employee's account will be checked again. If the employee still cannot access the system, then the team will **lose 1%** of the total possible SLA points.

The Blue team may reset the credentials of the employee's accounts and share them in Discord. Please reply to the initial message so the Black team can trigger a retest.
Red teams will not have access to these shared credentials. There is no need to write a formal report to the employee; just message the Black team.

Additional Information

- The same employee and system are tested across all teams.
- Tests are performed using the same level of access Blue teams have into the environment.
- If **four** or more warnings have been issued, then every additional will cost 0.5% of the total possible SLA points.
- Some checks take additional time to be performed by the Black team. Initial warning messages may be delayed; this will be accounted for when scoring.

NECCDC 2025 SEASON

PlaceboPharma is a publicly traded pharmaceutical company at the forefront of placebo research and innovation. Specializing in the production of high-quality placebo pills the company, and their business vendors, are dedicated to advancing the understanding of placebo effects through rigorous testing and data-driven analysis. Their state-of-the-art manufacturing facilities feature advanced machinery capable of producing quality controlling placebo pills at scale. Each machine is equipped with precision monitoring systems that record critical production metrics and experimental data. This information is continuously streamed into a hopefully secure and scalable database, enabling PlaceboPharma to monitor production, analyze trends and optimize manufacturing processes.

“At PlaceboPharma, our meds are so good, you'd swear they're real!”®

- Cybersecurity in Businesses
  - Risk Management
  - Business Value
- Data Processing
  - Handling of Sensitive Data
  - High Availability
- Infrastructure Monitoring
- Containerization // Orchestration
- Network Segmentation

Qualifier's Infrastructure

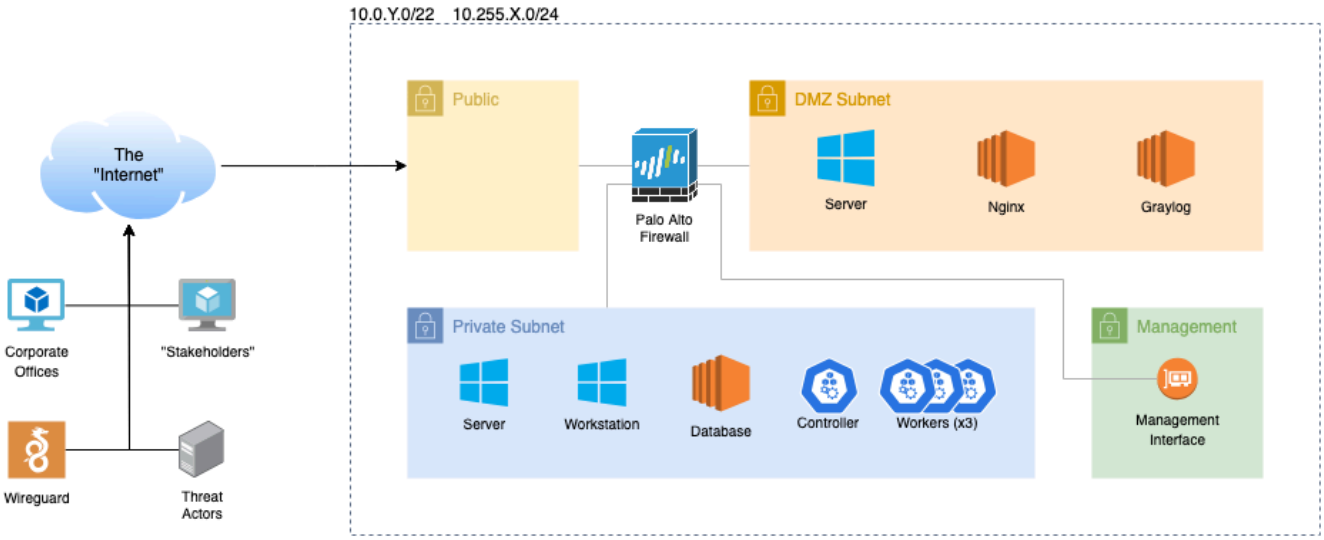
Contractors should be prepared to assess the various aspects of the organization's infrastructure. The primary objective is to maintain confidentiality of data while maintaining availability of PlaceboPharma production systems and employee access.

Technologies that may be found in the company's infrastructure include:

Windows Server*	Containerd	HAProxy
Microsoft Active Directory*	Docker	Nginx*
Certificate Authorities	Ubuntu	Traefik
Kerberos	Rocky Linux*	TSDB (InfluxDB*)
Kubernetes*	Palo Alto Firewall*	LongHorn
Open Source EMR	SQL	Graylog*
PowerPoint	Falco	Prometheus

*Confirmed services
AWS will not be in scope this year for the blue team

Additional infrastructure details will be provided by competition staff as we get closer to the date of the Qualifier through public channels.



Cybersecurity focuses on safeguarding the functions that drive business's value creation. Keep this in mind during the qualifiers competition.

Remote Access will be provided by Black Team to allow teams to connect to the Qualifier environment from their personal/campus computers and should be on an on-site location provided by their own educational institution.

Ensure you have **Wireguard** **installed** on machines used for competition **prior to the start** of the qualifiers competition. It is critical that teams use the beta period to validate they can connect to WireGuard instead of using precious time during the competition.

Black Team Operational Aid Charges

This year we've put together a quantitative document going over the point reduction for different Black Team operational assistance requests. Our goal behind this *Support Tax* is to balance between encouraging teams to seek help when genuinely needed and fostering independent problem-solving.

Point Pricing

Point reduction is only taken from the "SLA" portion of the points.The cost will be based on a percentage of the total possible SLA points. This way the same support impacts all teams evenly.

Type	Description / Example	Cost (%)
Server Redeployments	Cleanly redeploy the server to a pre-competition state. This will remove any changes performed by Blue or Red Teams.	2
Instance Network Restoration	This refers to removing firewall rules that block instance connectivity. Additionally, if the Black Team cannot restore access, a server redeployment may be required instead.	1.5
Account Logout	Password reset for any user (Blue, Black, Employee). If the Black Team cannot connect themselves, a server redeployment will be required instead.	1
Competent Questions	Thoughtful questions that include information on what your team has already tried, including results if applicable. Abuse of this offering or questions that lack any prior effort will result in a 0.5 point fee.	0
Competition Setup Questions	This includes questions related to initial environment VPN setup, access to initial credentials, questions designated to Black, White or Red Teams, and the like.	0

Additional Information

- When servers are redeployed or access is restored, teams do not get "refunded" the missing points they could have gained from Injects or scoring (SLA) checks.
- Server redeployments cannot be performed during the end of the competition.
- Make sure to use the **@BlackTeam** handle, otherwise your message will not be seen. Also keep in mind that the Black Team is also responding to other teams. If there is no response in five minutes, please ping us again.
- Upon request after competition completion, teams can request a summary of lost points.
- In case of *force majeure* or proven hosting issues, lost points can be refunded.
- The Black Team has full discretion to assign point pricing to help events.

Management Brief

Title: Ensuring Security and Efficiency at PlaceboPharma
Location: Bristol
Datetime: 2025-01-22 12:15:21

PlaceboPharma, a publicly traded pharmaceutical company specializing in the research, development, and production of high-quality placebo pills, is committed to advancing scientific understanding of placebo effects. As the company continues to grow, ensuring the security of its infrastructure, the integrity of sensitive data, and the optimization of manufacturing processes are top priorities.

As PlaceboPharma continues to innovate in the field of placebo research and scale up production, collaboration with third-party vendors and partners becomes an essential aspect of our operations. However, engaging with external entities introduces a range of risks, particularly in terms of cybersecurity, data integrity, and supply chain vulnerabilities. To mitigate these risks and safeguard our sensitive information and operational processes, PlaceboPharma has developed a comprehensive **Third-Party Risk Management Strategy**.

1. Vendor Selection and Due Diligence

Before entering into any agreements with third-party vendors, PlaceboPharma performs thorough due diligence to assess potential risks. This includes evaluating the following criteria:

- **Cybersecurity Policies**: All third-party vendors must demonstrate robust cybersecurity practices, including encryption, data protection measures, and incident response protocols. A detailed review of their security certifications is conducted to ensure compliance with industry standards.
- **Regulatory Compliance**: Vendors involved in pharmaceutical manufacturing, research, or data processing must adhere to the same stringent regulations that PlaceboPharma follows. HIPAA for patient data handling, and GDPR where applicable.
- **Business Continuity Plans**: Third-party vendors must provide a detailed business continuity and disaster recovery plan to demonstrate how they will maintain operations and recover data in the event of a failure, natural disaster, or cyberattack.
- **Performance Track Record**: We assess the reliability and past performance of vendors, particularly those involved in critical areas such as the supply chain, production facilities, and IT infrastructure.

2. Ongoing Monitoring and Risk Assessment

Once a third-party vendor is selected and onboarded, ongoing monitoring is essential to ensure they continue to meet PlaceboPharma's security and operational standards. Key elements of this ongoing monitoring include:

- **Continuous Risk Assessments and Security Audits**: Periodic re-assessments are performed to evaluate any changes in the vendor's operations, security posture, or financial stability that could impact PlaceboPharma's security or business continuity. This includes reviewing vendor risk reports and any updates on security incidents or breaches they may have experienced.
- **Security Audits**: Regular security audits are conducted to ensure that vendors are maintaining the necessary controls to protect sensitive data and infrastructure. These audits may be conducted by our internal security team or an external auditor to provide an unbiased review.
- **Access Control and Data Handling**: Any third-party vendor with access to PlaceboPharma's internal systems or sensitive data must follow strict access control protocols. This includes monitoring vendor activities within our systems and ensuring that their employees access only the data and systems necessary for their roles. Data exchange is securely encrypted, and we employ strict guidelines for data storage, retention, and destruction.

By implementing a comprehensive Third-Party Risk Strategy, PlaceboPharma not only mitigates the risks posed by external vendors but also strengthens its overall security posture and operational resilience. This strategy ensures that our third-party relationships are built on a foundation of trust, compliance, and continuous monitoring, helping us safeguard both our research and production processes. Through diligent vendor management and proactive risk mitigation, PlaceboPharma remains well-positioned to continue its leadership in placebo innovation, while minimizing potential disruptions from external sources.