PARTNERED WITH

MIDDLESEX Community College

IN COORDINATION WITH

NECCDL

PRESENTS THE

NORTHEAST COLLEGIATE CYBER DEFENSE COMPETITION

2026 SEASON QUALIFIER

BLUE TEAM PACKET

1.0.0 | 2026-12-19

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
Discord: discord.gg/rJn6DxwFTC

We would like to thank **Middlesex Community College** for being an outstanding partner for this season!

NECCDC 2026 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 2026 Qualifier is managed by 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.

This competition goes beyond just technical skill and is grounded in real-world business operations. Technical successes that impact business functions will lower a team's score, just as business-driven decisions that introduce security gaps can result in getting hacked.

Qualifying teams from the **NECCDC 2026 Qualifier on January 31, 2026** will have the opportunity to participate in the **NECCDC 2026 Regional**, expected to take place **Friday March 20 - Sunday March 22** at Middlesex Community College (33 Kearney Square, Lowell MA).

NECCDC 2026 Season Sponsors

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

Additional information regarding sponsorships for the NECCDC 2026 Season can be found at neccdl.org/sponsor and neccdl.org/history/2026.

Gold


Silver


HELP CONNECT US WITH POTENTIAL SPONSORS!
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

Highly recommended, but 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, Jan 24, 2026

TIME	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, and make sure they submit moderator contact information for training and coordination.

Saturday, 31 January, 2026

TIME	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/registration.html (due by Jan 19, 2026). Each competition team may consist of up to eight (8) members chosen from the submitted roster. In order to register with National CCDC, you must have at least four (4) members. For NECCDC, we will accept teams with less members as exhibition teams. 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 senior White Team 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 all teams must follow. There were some recent changes for the 2026 season that we request that you review in case you have been a longer-time participant in CCDC. It is possible that there may be additional changes as well, that we hope to communicate with you when / if they occur.

The list of published Blue Team script repositories will be available on the League's website once the registration deadline has passed.

- Besides the approved repositories, teams are **not** allowed to use **any private** materials.
- Review National CCDC rules (section 5) on internet and team supplied tool usage.
- 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. Questions can be asked in the NECCDL Discord as well and answers will be distributed across public channels.

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 (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 to reduce the impact of Red Team scoring.
- Ensure any executive summaries and business impact analyses are appropriately written for the intended audience (avoid 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.
- After an incident occurs, document the remediation steps clearly, including any actions taken to prevent it from happening again.
- Make sure that you include relevant screenshots, visuals and evidence.
- Think about whether what you are experiencing is really due to Red Team activity or due to a misconfiguration/actions taken by your team.

NECCDC 2026 SEASON

You and your team have recently been hired as security and operations engineers for ChefOps, a Managed Service Provider (MSP) focused on businesses in the food services industry. Their job is to protect both the company's internal infrastructure and that of a growing roster of clients.

As part of its initial contract, ChefOps has signed with Ocean Crest Kitchens, a regional chain undergoing a modernization of its legacy restaurant systems. Work items will focus on maintaining the core infrastructure of both Ocean Crest Kitchens and ChefOps, including monitoring, access management, and incident response, while navigating legacy systems.

- Change Management
  - Configuration Management
- Cybersecurity in Businesses
  - Business Value
  - Risk Management
- Identity and Access Control
  - Multi-Factor Authentication
- System Networking
- Monitoring and Alerting

Qualifier's Infrastructure

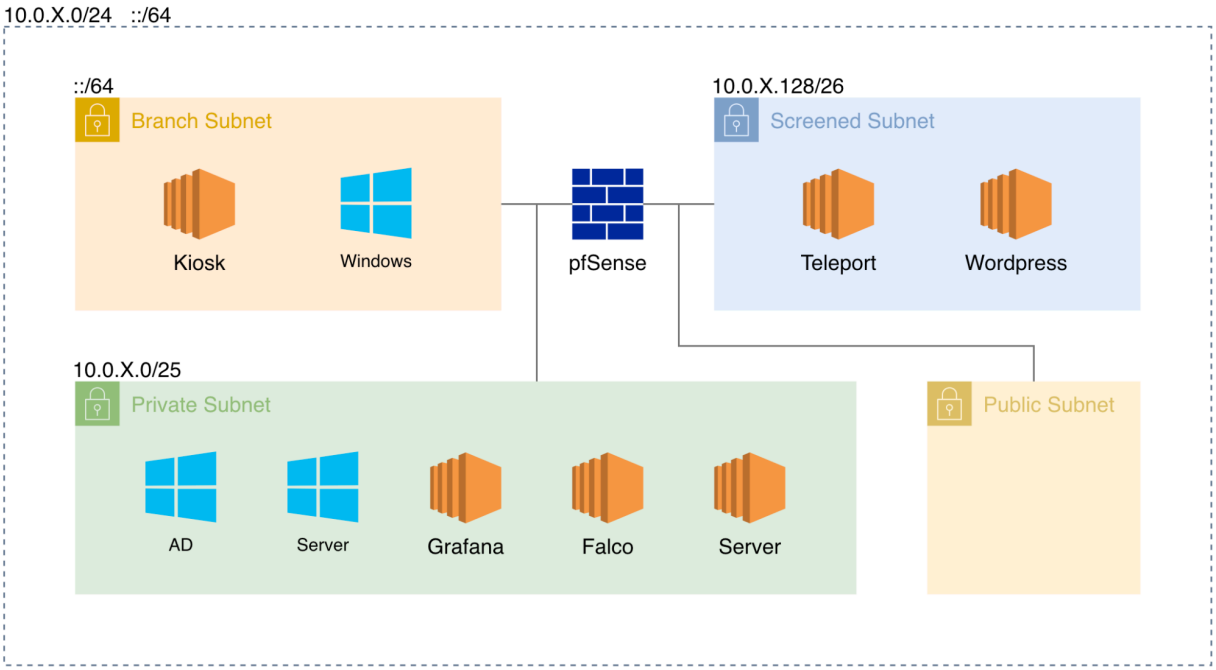
Teams should be prepared to assess the various aspects of the organization's infrastructure. The primary objective is to maintain the confidentiality, integrity and availability of ChefOps and its clients' production systems.

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

Active Directory*	Dual Stack	pfSense*
Alpine	Falco*	PowerPoint
Ansible	Federation	Prometheus
Centralized Logging	File Server	RHEL†*
Containerization	Grafana*	Teleport CE*
Database	Kiosk System	Windows Server*
Debian†*	Nginx	Wordpress*

*Confirmed services
† OS Family

Additional infrastructure details may 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 NECCDC competitions.

Remote Access will be provided by Black Team to allow teams to connect to the competition 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.

Operational Aid Charges

Teams are responsible for restoring their systems to operational status on their own, but sometimes this is not possible. The Black Team offers a point-based reduction to fix a system or provide assistance. The goal behind this change is to balance between encouraging teams to seek help when genuinely needed and fostering independent problem-solving.

Pricing Breakdown

Each team is given a budget of **1000 points** they can spend to request assistance from the Black Team. Spent points will only count against the system and **not inject** scoring.

Starting this season (2026), each assistance request **that has a point cost** will be multiplied by the corresponding number in the Fibonacci sequence (excluding 0). For example, the first request will cost x1, the second x1, the third x2, and so on, following the sequence of Fibonacci numbers.

Type	Description / Example	Cost
Server Redeployments Or Instance Connectivity Troubleshooting	Cleanly redeploy the server to a pre-competition state. Removing firewall rules that block instance connectivity, etc. If the Black Team cannot connect themselves, a server redeployment will likely be required instead.	30
Account Logout	Password reset for any user (Blue, Black, Employee). If the Black Team cannot connect themselves, a server redeployment will be required instead.	10
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 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 noticed. 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.
- The more point-costing requests you make to the Black Team for assistance, the higher the cost of each subsequent request.
- Upon request after competition completion, teams can request a summary of events that required the Black Teams intervention.
- 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.

Business 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, employees will be periodically checked to confirm they can continue performing their job functions by connecting to systems. These checks will involve individual employees and systems across all teams once the competition has started. Any action that renders a user or system inaccessible (red team tampering or blue team response) should be included in the incident response report.