
HOSTED BY



MIDDLESEX
Community College

IN COORDINATION WITH



PRESENTS THE

NORTHEAST COLLEGIATE CYBER DEFENSE COMPETITION

**2026 SEASON REGIONAL
BLUE TEAM PACKET**

v.1.0.0 | Revised 2026-02-27

CONTENTS

NORTHEAST COLLEGIATE CYBER DEFENSE LEAGUE	3
Competition Goals	3
Regionals Overview	4
NECCDC 2026 Season Sponsors	5
REGIONAL EVENT SCHEDULE	6
COMPETITION ORGANIZATION	7
Competition Rules	9
Competitor Authentication	9
Peripheral Devices	9
Questions and Answers	9
Scoring Overview	10
System Scoring	10
Inject Scoring	10
Red Team Activity	11
Incident Response Template	11
Tips for Effective IR Reports:	11
NECCDC 2026 SEASON	12
Regional's Infrastructure	12
Operational Aid Charges	13
Pricing Breakdown	13
Additional Information	14
Business Functions	14

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: neccd.org

GitHub: [NE-Collegiate-Cyber-Defense-League](https://github.com/NE-Collegiate-Cyber-Defense-League)

Follow on LinkedIn: [neccd](https://www.linkedin.com/company/neccd/)

Follow on Mastodon: [@neccd@infosec.exchange](https://infosec.exchange/@neccd/)

Follow on BlueSky: [@neccd.bsky.social](https://bsky.app/profile/neccd.bsky.social)

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

Regionals Overview

The NECCDC 2026 Regional is hosted by [Middlesex Community College](#), 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.

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

The winning team from the NECCDC 2026 Regional on **March 20-22, 2026**, will advance to the [CCDC National Championship](#). The second-place team will have the opportunity to compete in a wildcard competition for a spot in nationals.

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 neccd.org/sponsor and neccd.org/history/2026.

PLATINUM
 <p>STRENGTHENING COMMUNITY COLLEGES TRAINING GRANTS</p>

GOLD


SILVER






OTHERS? HELP CONNECT US WITH POTENTIAL SPONSORS!

Let us know if you have someone you know who is interested in sponsoring!
Have them contact sponsor@neccd.org for more information.

REGIONAL EVENT SCHEDULE

Friday, March 20	Event	Location
8:00 - 9:00	Check In (Name tags & release forms)	Front Desk
8:00 - 9:00	Breakfast (informal breakout)	Lower Cafe/Upper Cafe
9:00 - 9:30	Competition Opening Ceremony	Lower Cafe
9:30 - 10:00	Teams Staging to Rooms	Floors 2, 3 & 4
10:00 - 16:00	NECCDC Student Competition	Floors 1 & 2
12:00 - 12:45	Lunch	Lower Cafe/Upper Cafe
16:00 -	Dinner on your Own w/ Team	

Saturday, March 21	Event	Location
8:00 - 9:00	Breakfast + General Info/ Recap	Lower Cafe/Upper Cafe
9:30 - 10:00	Teams Staging to Rooms	Floors 2, 3 & 4
9:30 - 14:30	NECCDC Student Competition	Floors 1 & 2
12:00 - 12:45	Lunch	Lower Cafe/Upper Cafe
12:00 - 14:30	TBD	Lower Cafe/Upper Cafe
14:30 - 16:00	Cybersecurity Panel	Lower Cafe/Upper Cafe
17:00 - 19:00	Dinner (Buffet)	Lower Cafe/Upper Cafe
17:00 - 19:00	Recruitment Event	TBD

Sunday, March 22	Event	Location
8:00 - 10:30	Full Breakfast	Lower Cafe/Upper Cafe
9:00 - 10:30	Exercise	Lower Cafe/Upper Cafe
10:30 - 10:45	Break	Lower Cafe/Upper Cafe
10:45 - 11:30	Debriefs Red/Black/White	Lower Cafe/Upper Cafe
11:30 - 12:00	Closing & Awards Ceremonies	Lower Cafe/Upper Cafe

COMPETITION ORGANIZATION

Blue Team

Student team representing a specific academic institution or major campus competing in the NECCDC. Each competition team may consist of up to eight (8) members chosen from the submitted roster. The remainder of the roster is for substitution if a member of the active competition team cannot compete. This list of up to 12 is set as of January 31, 2026 (Start of NECCDC Qualifiers). On each day, only eight competitors may be in the team room at one time and cannot be changed during the day. Substitution after the competition starts each day in the competition team requires approval from the Competition Staff.

- 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 team members are qualified for participation.
- If there are **technical issues**, open a ticket and **@BlackTeam** for infrastructure-related questions. If competitors are unsure about **other questions**, then they should ask their room moderators.

Black Team

Black Team members are our competition technicians. They develop, deploy, and maintain a unique competition environment every year. They also configure remote access, Discord, the service scoring engine, and help write technical injects alongside the White Team.

White Team

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

- Moderators are responsible for performing tasks such as:
 - Undertake/Review moderator training offered by NECCDC
 - Gain familiarity with 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
 - 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 concerning scoring. The chief judge has no active or historical, professional or personal affiliation with any school in the league.

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 may also include individuals who act as employees, clients, or other external 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, but we also truly strive to create a fun and safe professional and technical learning environment every year.

Competitor Authentication

Competitors will be expected to show a valid/current student ID (can be through official digital ID app or physical card), issued by their educational institution, to authenticate during check-in. Authentication will be done by registration desk staff and in-room moderators.

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

Peripheral Devices

Competitors are permitted to use their own peripheral devices, including mice, keyboards, headphones, etc. However, to use such devices, please submit a formal request to blackteam@neccd.org for pre-approval **at least one week in advance** of the competition. Please include any relevant device information, such as name, brand, and model number, as well as photographs.

If any participant requires specific devices for special accommodations or medical reasons, please communicate this in the formal request. Approved devices will be recorded.

All devices will be subject to a daily vetting process by the Black Team at the start of each competition day. Keyboards and mice will already be provided to each team.

Questions and Answers

We maintain a set of Questions and Answers from our information sessions, publicly available on the [website](#). If there are additional questions, reach out in the League [Discord](#) or [email](#) us.

Scoring Overview

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

50%	System Scoring
50%	Inject Scoring

Service uptime and inject completion have equal scoring weights. 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, a 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 at 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 2026 Season - Black Team Operational Aid Charges below).

Inject Scoring

Injects are business tasks that are 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 the Blue Team's 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 Response (IR) 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). [Red team advice](#).

Incident Response Template

Please feel free to use this Incident Response (IR) [Template](#), or use a similar professional report that captures data referenced in [National Rules 9.d](#). See this [sample](#) IR executive summary.

Tips for Effective IR Reports:

- Submit reports when incidents occur to reduce future Red Team impacts. If the report is accurate in reporting the Red Team Activity, the points lost due to the Red Team activity can be recovered.
- 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 the report 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.

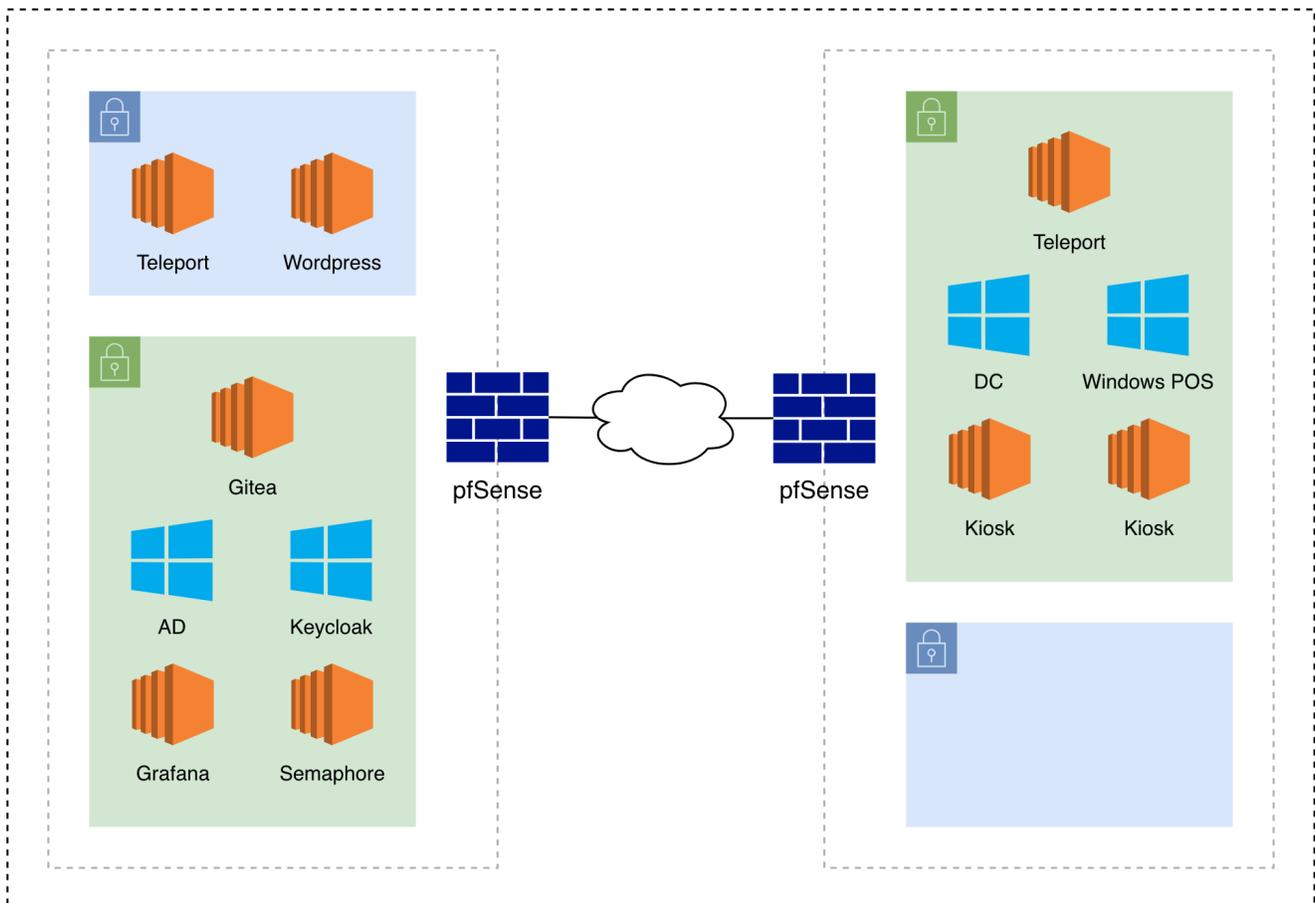
NECCDC 2026 SEASON

You and your team were recently 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.

Since Ocean Crest Kitchens became a client, your team has upgraded its internal networks and integrated them into ChefOps core infrastructure. Work items will continue to focus on maintaining the security of core infrastructure and monitoring new and legacy systems.

Regional'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' networks and systems.



Additional infrastructure details may be provided by competition staff as we get closer to the date of the regional 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** that they can spend on 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](#)” for the missing points they could have gained from Injects or scoring (SLA) checks.
- Server redeployments cannot be performed during the end of the competition.
- Submit a ticket and 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. Each check will be performed randomly across all teams and will only involve one employee and one system. Each occurrence of an employee not being able to connect will result in **5 points** deducted from the team's operational support budget (does not exponentially scale).

Teams can recoup points from a failed check if the following criteria are true:

1. An incident report is submitted explaining the root cause
2. Activity is confirmed by the red team
3. Is an appropriate DFIR action