

HOSTED BY



IN COORDINATION WITH



PRESENTS THE

NORTHEAST COLLEGIATE CYBER DEFENSE COMPETITION

2025 SEASON REGIONAL BLUE TEAM PACKET

v.1.0.0 | Revised 2025-02-17

CONTENTS

NORTHEAST COLLEGIATE CYBER DEFENSE LEAGUE	3
Competition Goals	3
Regionals Overview	4
NECCDC 2025 Season Sponsors	5
REGIONAL EVENT SCHEDULE	7
COMPETITION ORGANIZATION	8
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
PlaceboPharma Employee Job Functions	12
Additional Information	12
NECCDC 2025 SEASON	13
Regional's Infrastructure	13
Technology Changes	13
Black Team Operational Aid Charges	14
Point Pricing	14
Management Brief	16

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

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

Follow on LinkedIn: [northeast-collegiate-cyber-defense-league](https://www.linkedin.com/company/northeast-collegiate-cyber-defense-league)

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

Follow on BlueSky: [@neccdl.bsky.social](https://bsky.social/neccdl)

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

Regionals Overview

The NECCDC 2025 Regional is hosted 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.

The winning team from the NECCDC 2025 Regional on March 14-16, 2025 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 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 neccd.org/sponsor and neccd.org/history/2025.

PLATINUM	
	
	
GOLD	
	
<p>Donation from Raytheon Alum</p>	
SILVER	
	
	



BRONZE

FORTRA
Cobalt Strike

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@neccdl.org for more information.

REGIONAL EVENT SCHEDULE

Friday, March 14	Event	Location
8:00 am - 9:00 am	Check In (Name tags & release forms)	GHH Main Level (Floor 1)
8:00 am - 9:00 am	Breakfast (informal breakout)	
9:00 am - 9:30 am	Competition Opening Ceremony	GHH Atrium (Lower level)
9:30 am - 10:00 am	Teams Staging to Rooms	
10:00 am - 4:00 pm	NECCDC Student Competition	Levels 0, 1, 2
12:00 pm - 12:45 pm	Team Lunch	GHH Main Atrium
Saturday, March 15	Event	Location
8:00 am - 9:00 am	Breakfast	GHH Atrium (Lower level)
8:30 am - 9:00 am	Day 02 Debrief	GHH Atrium (Lower level)
9:30 am - 3:00 pm	NECCDC Student Competition	Levels 0, 1, 2
12:00 pm - 1:00 pm	Coaches' Meeting	Room G01 (GHH lower level)
12:00 pm - 12:45 pm	Team Lunch	GHH Main Atrium
5:00 pm - 8:00 pm	Recruitment Event, Dinner	GHH Atrium (Lower level)
Sunday, March 16	Event	Location
8:30 am - 9:30 am	Continental Breakfast	GHH Main Atrium
9:30 am - 11:30 am	Debriefs White/Red/Black	GHH Main Atrium
11:30 am - 12:30 pm	Awards Ceremonies	GHH Main Atrium
12:30 pm - 2:00 pm	Networking / Socializing	GHH Main Atrium

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 in the event a member of the active competition team cannot compete. This list of up to 12 is set as of February 1, 2025 (Start of NECCDC Qualifiers). On each day, only eight competitors may be in any team room at one time and cannot be changed during the day. Substitution anytime after the competition starts each day 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.

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.

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.

- 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

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.

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 the check-in. Authentication will be done by registration desk staff / in-room moderators.

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.

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@neccdl.org** for pre-approval **at least one (1) week in advance** of the competition. Please include any relevant device information, e.g., brand, model number, as well as photographs.

If any participant requires specific devices due to 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 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 periodically 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 check, the previously failed employee's account will be checked again. If the employee still cannot access the system, then the team will lose a small portion of 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 warning will cost the team. This is to prevent gaming the system.
- 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.
- If credentials are changed before the employee attempts to access a system this will still count as a warning.

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 secure database, enabling PlaceboPharma to monitor production, analyze trends and optimize manufacturing processes.

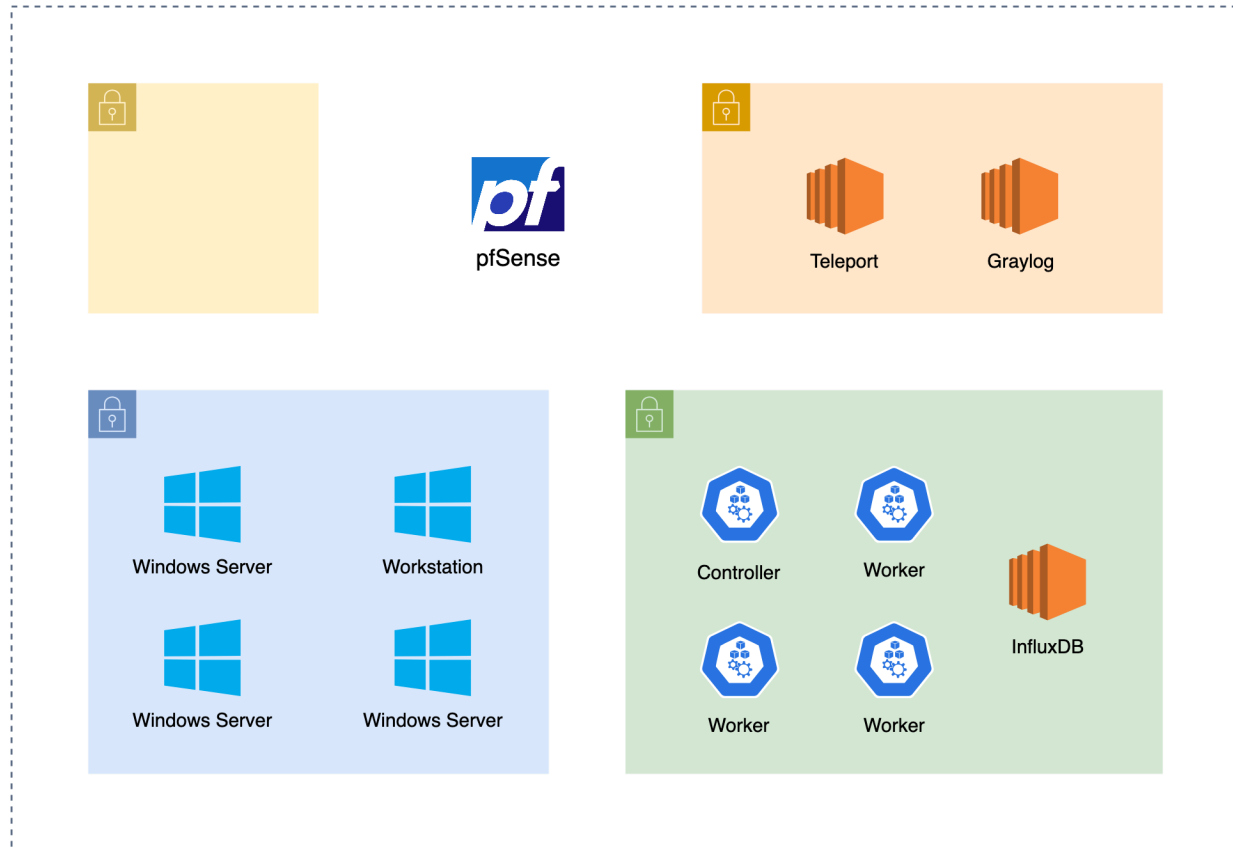
Regional's Infrastructure

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

Technology Changes

- [Teleport](#) will be introduced into the PlaceboPharma infrastructure
- The PlaceboPharma network administrators have **replaced** the **Palo Alto** infrastructure with a **pfSense firewall**.
 - We ran into intermittent issues during deployments, and will explain this fully in a [blog post](#) after the season is over. [TL;WR](#)

Additional infrastructure details may be provided by competition staff as we get closer to the date of the regionals competition.



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

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

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.

- Teams can request an in-person visit instead of addressing the issue over Discord.
- Server redeployments cannot be performed during the end of the second day.

- 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.
- 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 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.

Type	Description / Example	Cost
Server Redeployments	Cleanly redeploy the server to a pre-competition state.	20
Instance Network Restoration	Removing firewall rules that block instance connectivity. Additionally, if the Black Team cannot connect themselves, a server redeployment will likely be required instead.	15
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

Management Brief

Title: PlaceboPharma M&A Update

Location: Bristol, RI USA

Datetime: 2025-2-20 10:14:36

Origin and Growth: PlaceboPharma's journey to becoming a leader in pharmaceutical innovation began over two decades ago when its founder, Dr. Evelyn Turner, a renowned neuroscientist, realized the untapped potential of placebo effects in clinical trials. Initially starting as a small research lab, PlaceboPharma's mission was to bridge the gap between science and human perception, focusing on developing high-quality placebo pills that could provide reliable and reproducible results in experimental settings. In its early years, the company faced skepticism and financial uncertainty, but Dr. Turner's groundbreaking studies on placebo-driven therapeutic outcomes began to attract the attention of top medical researchers and investors. By partnering with major academic institutions and securing patents for proprietary manufacturing techniques, PlaceboPharma rapidly expanded, securing contracts with global pharmaceutical companies. Through relentless innovation, cutting-edge technology, and an unwavering commitment to data-driven research, PlaceboPharma revolutionized the placebo sector, eventually becoming a publicly traded powerhouse in the global pharmaceutical industry. Today, the company is not only a leader in placebo research but also a trusted partner for clinical trials, reshaping how the medical world understands the power of perception in healing.

Recent Developments: In a significant move that marks a new chapter in its history, PlaceboPharma recently announced its acquisition of IllusioPharma, a company known for its focus on developing placebo-based digital therapeutics. This strategic merger combines PlaceboPharma's expertise in pharmaceutical innovation and clinical trials with IllusioPharma's cutting-edge technology in virtual placebo experiences. Together, the unified entity aims to explore new dimensions in placebo-driven therapies, from traditional pharmaceutical applications to emerging digital health solutions. The merger strengthens PlaceboPharma's position in the global market and provides opportunities to diversify its offerings and enhance its research capabilities. The combined resources and expertise promise to revolutionize how the industry approaches the integration of perception, technology, and healing.

Rivalry and Acquisition: PlaceboPharma operates in a competitive landscape with several companies vying for dominance in the placebo and alternative therapies market. One of its main competitors, SimulacraMed, specializes in creating synthetic placebo treatments designed to mimic real pharmaceuticals, though their methods have been criticized for lack of transparency in their clinical trial data. Another rival, Biotechnica, has gained attention for its aggressive marketing tactics, claiming to enhance placebo effects through advanced

neurostimulation devices, but their products have faced regulatory hurdles and concerns over safety. While IllusioPharma previously competed in the digital therapeutics space, its merger with PlaceboPharma eliminates a key competitor and brings advanced capabilities under one roof. Despite these competitors, PlaceboPharma's commitment to rigorous scientific research, transparent data practices, and cutting-edge manufacturing technologies has helped it maintain a leading position in the industry, setting it apart from the more speculative, unproven, and dangerous approaches of its rivals.

Integration and Challenges: While PlaceboPharma works closely with a select group of trusted third-party vendors to support its manufacturing and data analytics operations, the company recognizes several potential risks associated with these partnerships. These risks include the possibility of supply chain disruptions, data security vulnerabilities, and quality control inconsistencies. Third-party vendors responsible for key components, such as raw materials and precision monitoring systems, may face challenges that could affect the timely delivery of materials or the reliability of data streams. Furthermore, as the company relies heavily on third-party vendors for maintaining secure and scalable database infrastructure, there is an inherent risk of cybersecurity breaches, which could compromise sensitive production data, documentation, and proprietary research. PlaceboPharma is committed to mitigating these risks through comprehensive vendor assessments, stringent contractual safeguards, and proactive monitoring, yet acknowledges the potential impact these factors could have on production timelines and overall business continuity. The merger with IllusioPharma also presents integration challenges, including aligning corporate cultures, streamlining operations, and ensuring consistent quality standards across the newly expanded organization.

Cybersecurity Overhaul: As PlaceboPharma continues to expand its operations globally, the company faces increasing challenges in managing the risks associated with its third-party vendors. While the company has historically relied on a network of trusted partners for critical supply chain components and data management, recent incidents have highlighted the need for a comprehensive overhaul of its third-party risk management practices. Issues such as delayed deliveries of raw materials, security breaches in vendor-managed databases, and inconsistent quality control from suppliers have raised concerns about the reliability of its external relationships. To address these vulnerabilities, PlaceboPharma recognizes the need for a more robust and proactive approach, which includes establishing stricter vetting procedures, enhancing monitoring systems, and implementing more stringent contract terms to ensure vendor compliance. The company also plans to invest in advanced cybersecurity measures to safeguard sensitive data and reduce the risk of potential breaches. By strengthening its third-party risk management framework and incorporating IllusioPharma's technological expertise, PlaceboPharma aims to secure its supply chain, protect its proprietary research, and maintain the high standards of excellence that have made it a leader in the pharmaceutical industry.