

# NECCDC 2025



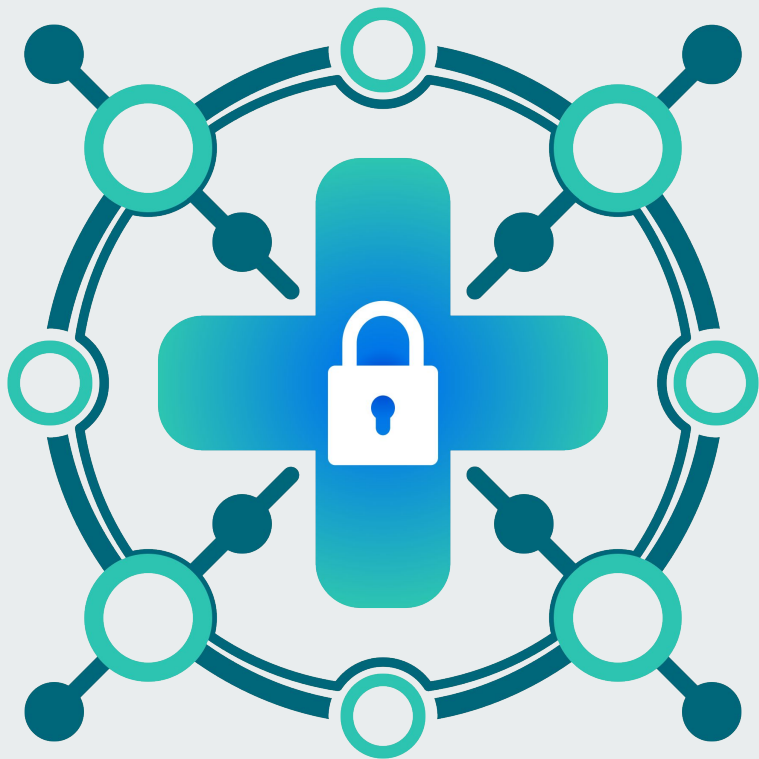
**Northeast Collegiate  
Cyber Defense  
Competition**

**RWU**  
Roger Williams  
UNIVERSITY



# Welcome

- General Overview
- Black Team Overview
- White Team Overview
- Red Team Overview
- Logistics & Schedules
- Sponsors



# NECCDC 2025 General Overview



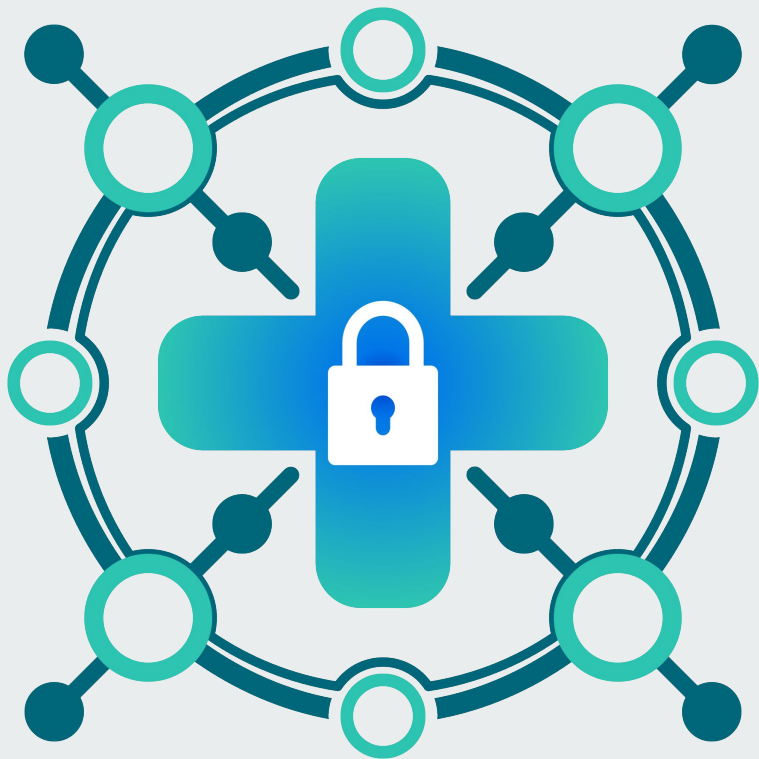
## Competition Theme

Third-party risk management is vital in healthcare to protect patient data and ensure compliance with regulations like HIPAA and HITECH. With increased reliance on external vendors for services like cloud storage and IT support, healthcare organizations face risks such as cyberattacks and data breaches. Effective management involves assessing vendors' security practices, robust contract management, and continuous monitoring to mitigate vulnerabilities, safeguard privacy, and maintain trust.



## Competition Scenario

**PlaceboPharma** is a leading pharmaceutical company specializing in placebo research and production. They focus on advancing the understanding of placebo effects through rigorous testing and data analysis. Their advanced manufacturing facilities produce placebo pills at scale, using precision monitoring systems to record critical production metrics. This data is securely stored in a scalable database, allowing for real-time monitoring, trend analysis, and process optimization.



**NECCDC**

**2025**

**Black Team**

**Overview**



## Environment Themes

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

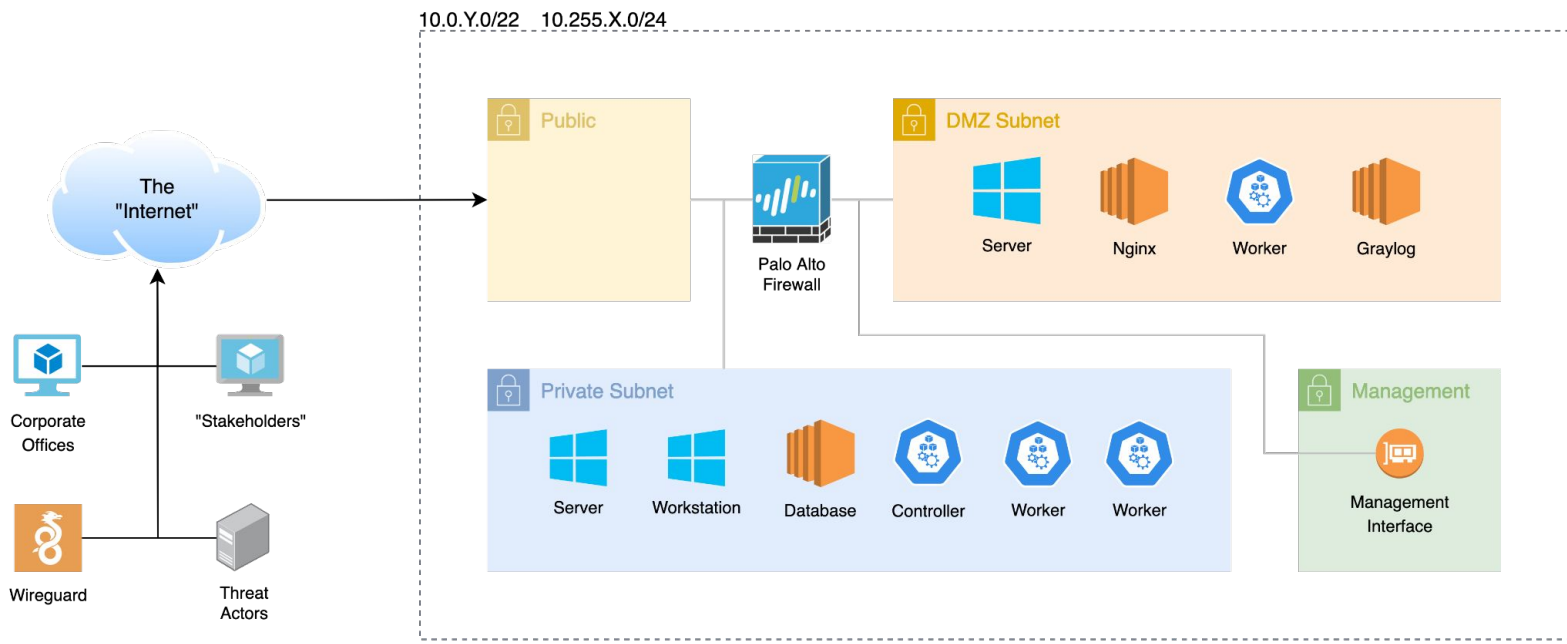


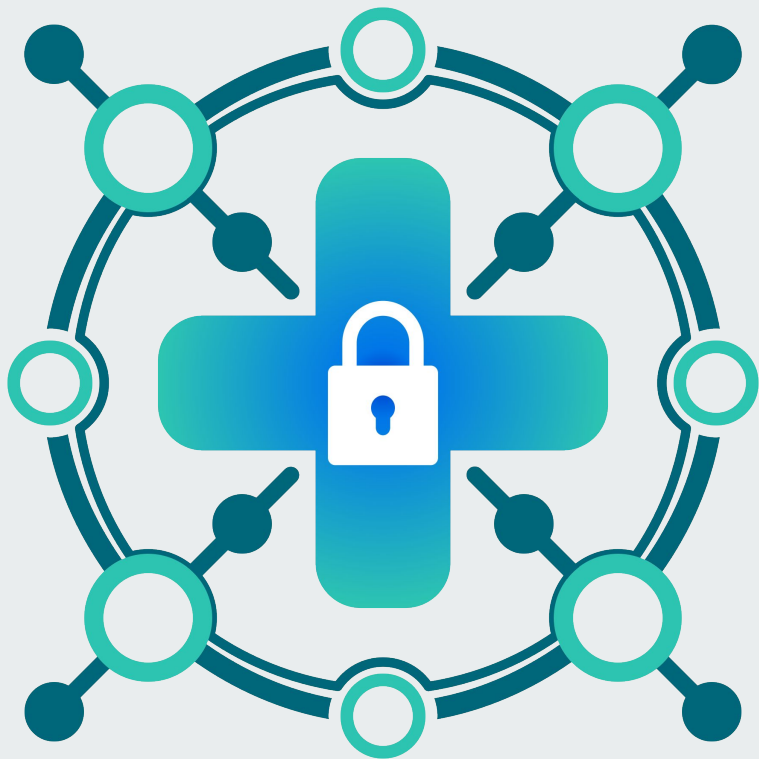
# Infrastructure Services

- Data Pipelines
- Gateway API
- Graylog
- InfluxDB
- Kubernetes
- Microsoft Active Directory
- nginx
- Palo Alto Firewalls
- Rocky Linux
- Windows Server



# Network Diagram





# NECCDC 2025 White Team Overview



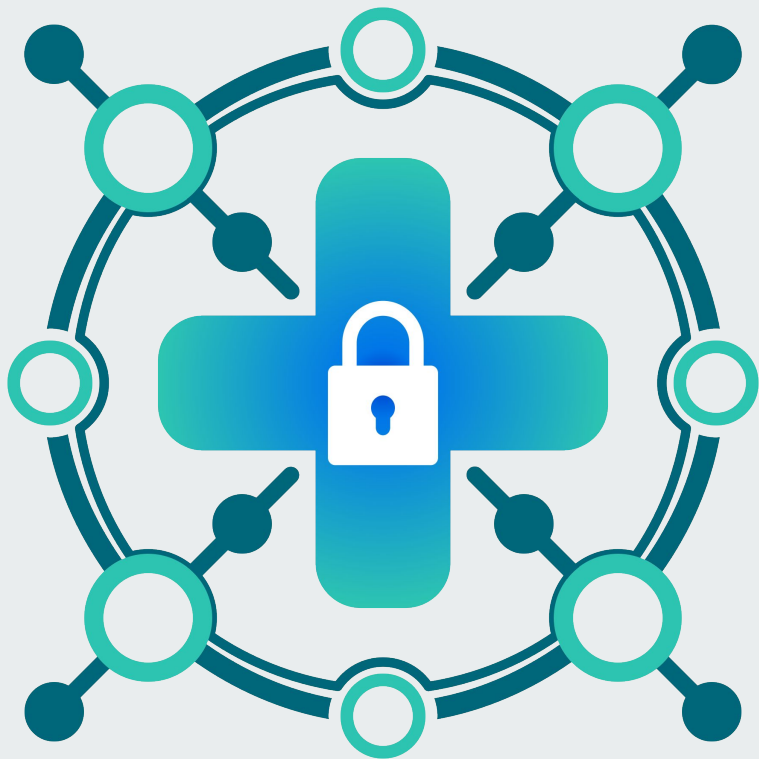
## Inject Advice

- Read / re-read directions & instructions → most answers are there!
- If inject requests executive summary → include one (remember audience)
- Ensure you submit correct & timely evidence of what was accomplished
- Not everything that anyone asks for is ok - think security & impact on mission
- Change your default passwords!
- Become familiar with game tech & infrastructure
- Pay attention to **@neccdl LinkedIn/X/Twitter/Mastodon** & current events
- Any questions re: inject or need clarification or if you have a situation occur beyond your control that affects your inject submission:
  - Ask your moderator(s) to intercede on your behalf to @WhiteTeam - if you don't ask, they won't



## Teamwork / Leadership Advice

- Know hierarchy for skills / knowledge & delegate tasks appropriately
- Encourage verbal communication with all team members
- Leaders should check-in regularly with team & leverage ideas while not micro-managing
- Use your tools, e.g. Discord team channel for organization
- Have contingency plans in place for loss of services
- Be calm, remain professional & have a good attitude under pressure
- Eat & hydrate - your brain needs energy to work. :) - also feed the mods!



# NECCDC 2025 Red Team Overview



## Red Team Advice

- Who ever has the most fun, wins - *Dan B.*
- Develop good teamwork & team support
- Find teammates that you enjoy working with under pressure!
- Be a teammate that others enjoy working with under pressure!
- Read the “[2025 Red Team Advice](#)” PDF
  - \* Posted in Resources after presentation



## IR Reports

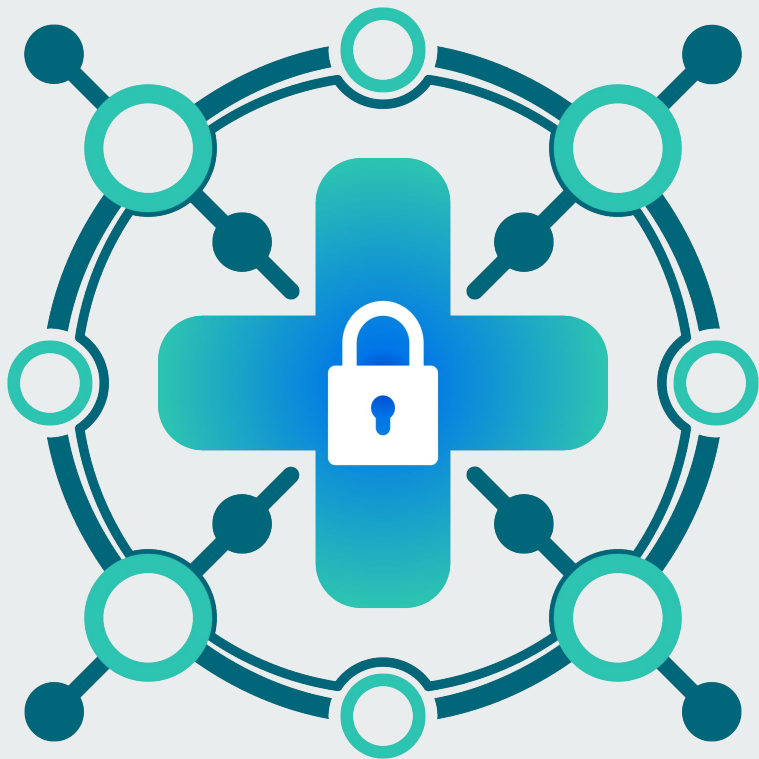
- Submit good IR reports when incidents occur to reduce Red Team scoring impact
- Ensure professionalism when writing and enough necessary information & depth to describe the incident and business impact
- Ensure executive summaries and business impact analyses are written for the intended audience. Minimize the technical jargon in these sections of the report
- Ensure that you accurately identify the business impact



## IR Reports

- Attempt to accurately determine the root cause
- Once an incident has been discovered, determine root cause & perform remediation. Any actions taken towards remediation/prevention should be detailed in the report
- Make sure you include relevant screenshots, visuals, and evidence
- Is what you are experiencing really due to Red Team activity or is it misconfiguration or actions by your own team?





**NECCDC**  
**2025**  
**Logistics &**  
**Schedules**



## Key Dates of the Season

- Sign-up to join the league is open: <https://neccdl.org/join>
- **January 24, 2025:** NECCDC 2025 Roster Submission Deadline
  - The earlier teams are registered, the sooner they have access to resources & Discord
- **January 25, 2025:** Qualifier Beta Test



## Key Dates of the Season

- February 01, 2025: NECCDC 2025 Qualifier
- TBD Mid-February 2025: Quals Outbrief & Regional Overview
- March 14-16, 2025: NECCDC 2025 Regional Onsite at RWU
  - 10 Teams who qualify will compete for who will advance to Nationals
  - League Member Institution Delegates (Coaches) will meet to discuss future NECCDL topics



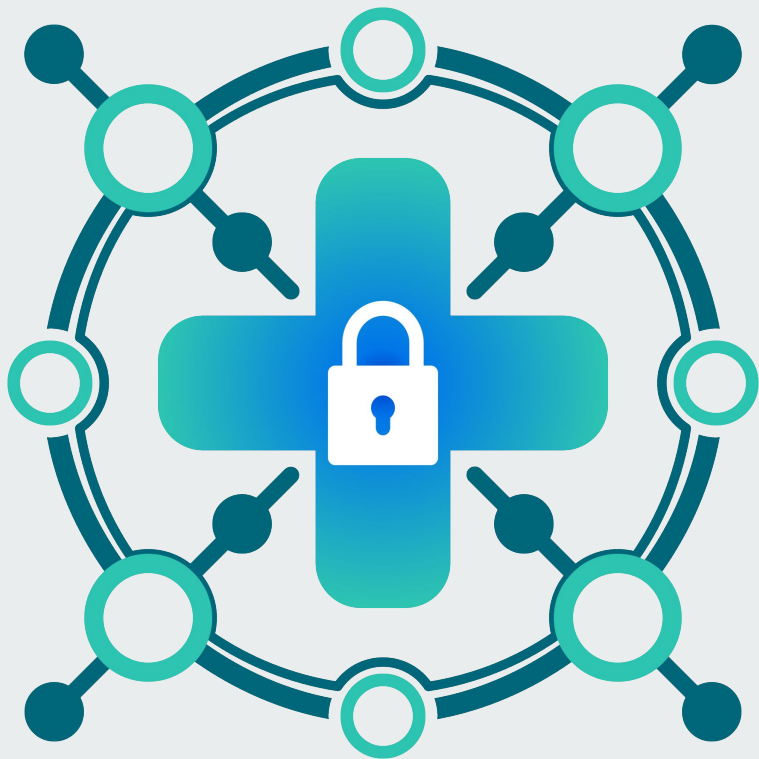
## Qualifier Schedule

TIME (EST)	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.



## Resources

- <https://neccd.org/history/2025/#resources>
- [NECCDC 2025 Qualifiers Packet](#)
- [2025 Red Team Advice](#)



**NECCDC  
2025  
Sponsors**

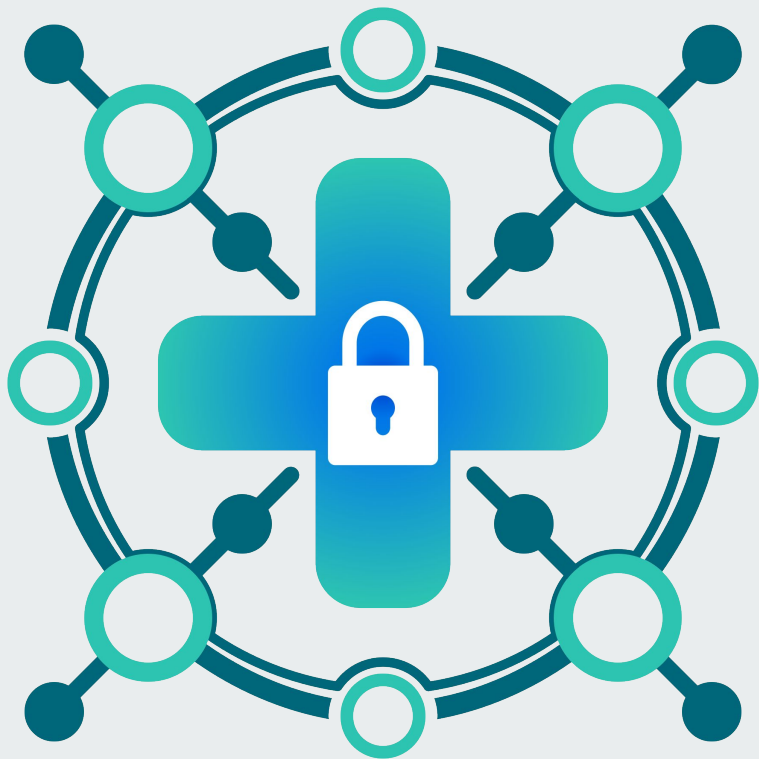
# NECCDC 2025 Current Sponsors



Also thanks to a Raytheon Alum for their generous gift at the Gold level!



Please reach out at: [sponsor@neccd.org](mailto:sponsor@neccd.org) with contacts/recommendations for sponsors!



**Q&A**