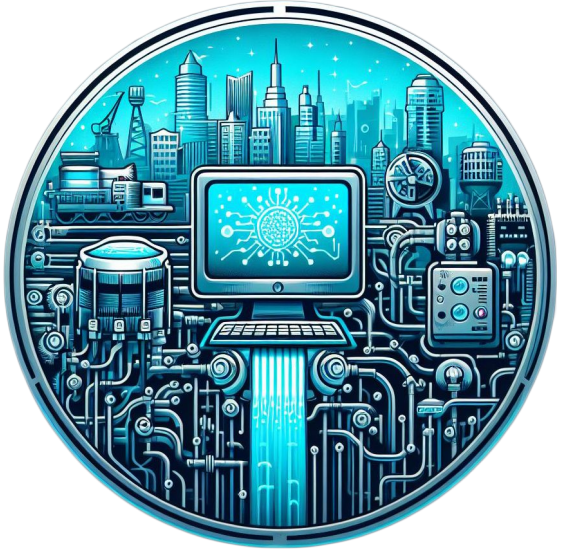
NORTHEAST COLLEGIATE CYBER DEFENSE COMPETITION (NECCDC) 2024



CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

Qualifier: Feb 3, 2024

Regional: Mar 23 – 25 2024

Hosted by

PACE UNIVERSITY

In Coordination with

NECCDL

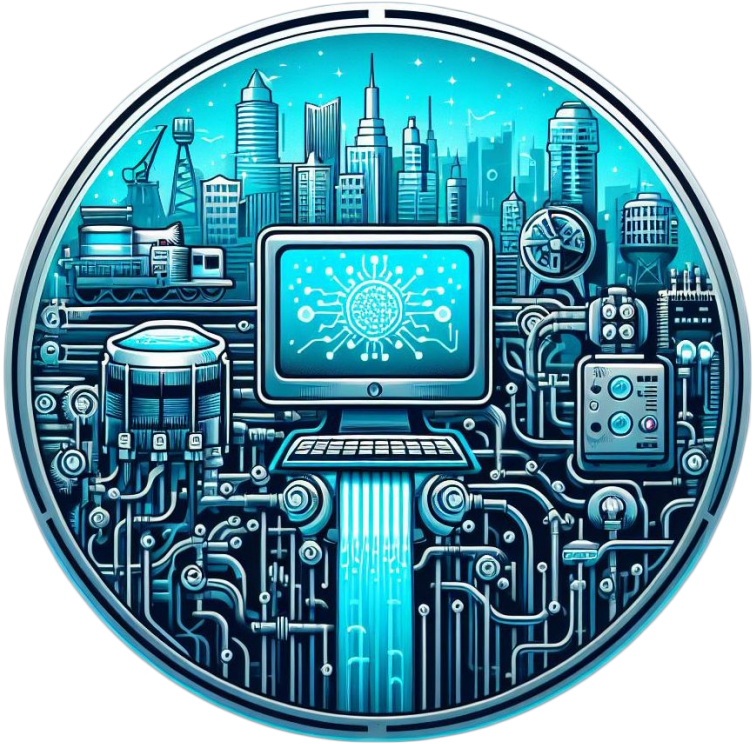
In Partnership with

NSF

Raytheon Technologies

NECCDC 2024 Welcome

- General Overview
- Black Team Overview
- White Team Overview
- Red Team Overview
- Logistics & Schedules
- Sponsors
- Please hold questions until Q&A



CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

NECCDC 2024 General Overview

NECCDC 2024 Theme

Critical Controls, Protecting our Infrastructure

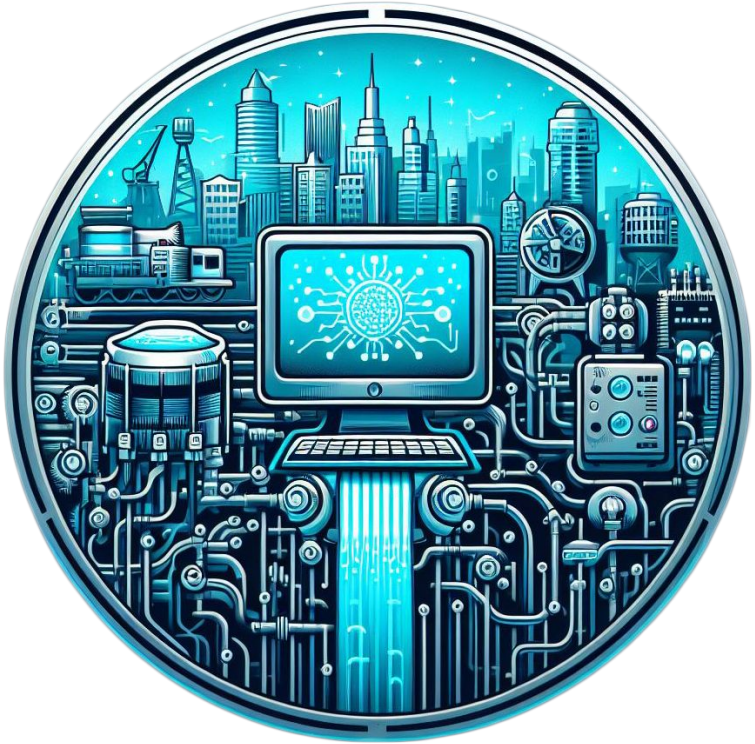
Critical infrastructure, which includes power grids, water systems, transport networks, and healthcare facilities, is pivotal to our nation's operation. Cyberattacks on these systems can not only disrupt daily life and endanger national security but also have profound economic and social implications. These infrastructures often blend **IT** with **OT** to boost production and meet demands, presenting a unique cybersecurity challenge. While defending the established **IT** domain is already demanding, protecting the less-prepared **OT** environment intensifies the task, with both tangible and intangible damages at stake.

NECCDC 2024 Scenario

Private energy company recently acquired another energy company that has significant critical infrastructure investments in the renewable energy sector including ownership of a hydroelectric dam.

Discovering that the cybersecurity oversight of especially the IT/OT aspects as well as general understaffing and risk management was poorly performed, the company engaged a preliminary assessment team to determine priorities.

It is now hiring an elite team of cyber security engineers to their Cascade Falls Dam location.



CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

NECCDC 2024 Black Team Overview

NECCDC 2024 Core Foci

- General
  - Resiliency
  - High Availability
  - Vulnerability Management
  - Endpoint Security
- Identity Management
  - Active Directory
  - RHEL IDM
- Containerization
  - Kubernetes
  - Containerd / Docker
- Additional Technologies
  - Ansible
  - Secrets/Credential Management
  - SIEM (Wazuh)

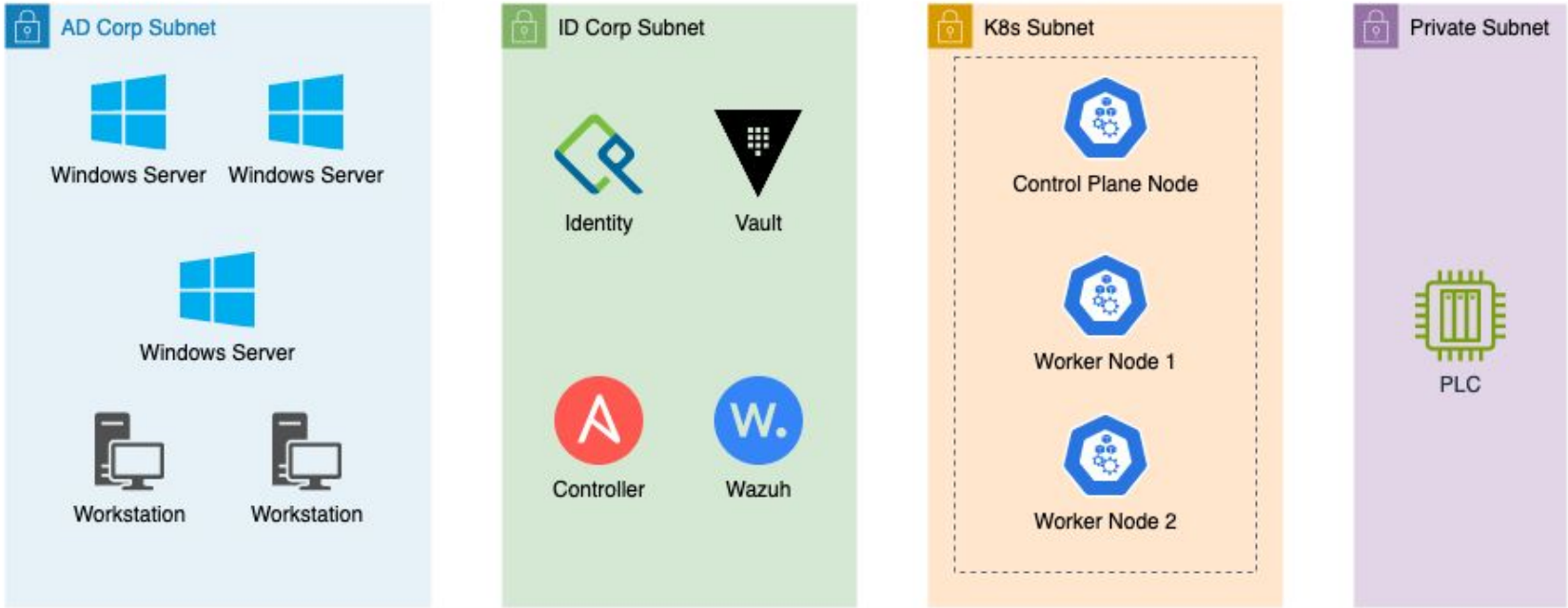
*Kubernetes is not a containerization tool

NECCDC 2024 Services

- Confirmed Services
  - Red Hat Identity Management (IdM)
  - Kubernetes
  - HashiCorp Vault
  - Semaphore

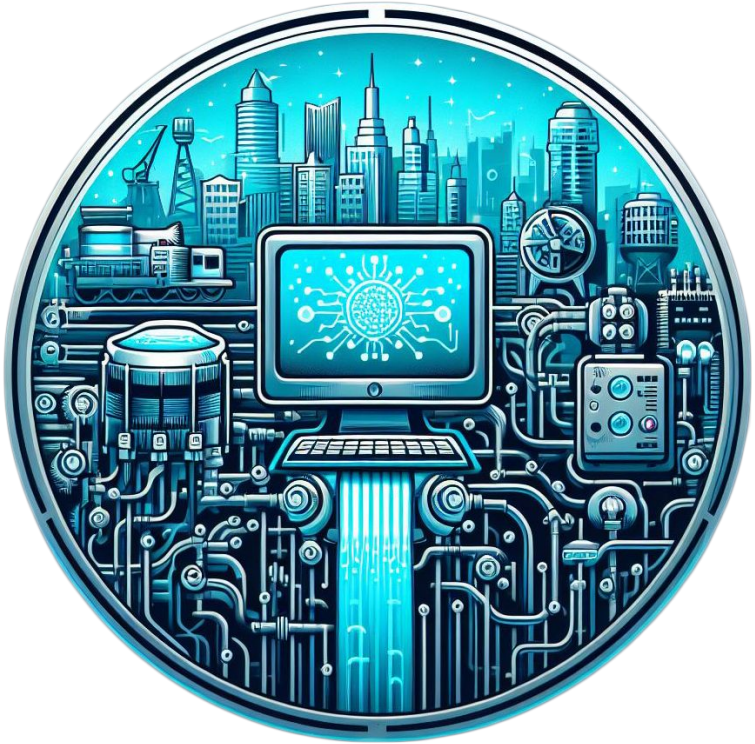
- Confirmed K8s Services
  - PostgreSQL
  - GitLab

NECCDC 2024 High Level Network Architecture



NECCDC 2024 | Black Team CTF

- Black Team is offering CTF-style challenges with hidden “hints” (if you pay close attention)
- Generally offered every Friday via our X/Twitter @neccdl & Mastodon @neccdl@infosec.exchange
- Solutions made available to those who have either joined the league (and paid the league membership fee) and/or registered at Nationals (resumes & rosters)
- Contact blackteamctf@neccdl.org with questions



CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

NECCDC 2024 White Team Overview

NECCDC 2024 White Team Guidance - Injects

- 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 in infrastructure (e.g., Waz*uh*)
- Pay attention to **@neccdl X/Twitter /Mastodon** & current events (*hints*)
- 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

NECCDC 2024 White Team Guidance - Teamwork

- 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!

CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

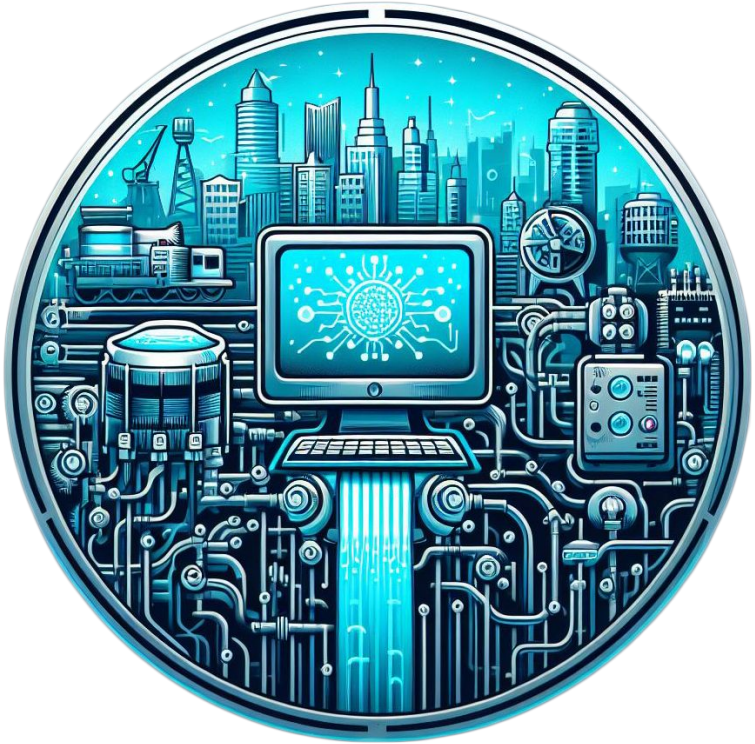
NECCDC 2024 Red Team Overview

NECCDC 2024 General Advice from Red Team

- 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 “2024 Red Team Advice” PDF
- See Rule 1

NECCDC 2024 Red Team Tips for Effective 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
- Attempt to accurately determine the root cause
- Once an incident has been discovered, determine root cause 7 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?



CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

NECCDC 2024 Logistics & Schedules

NECCDC 2024 Key Dates

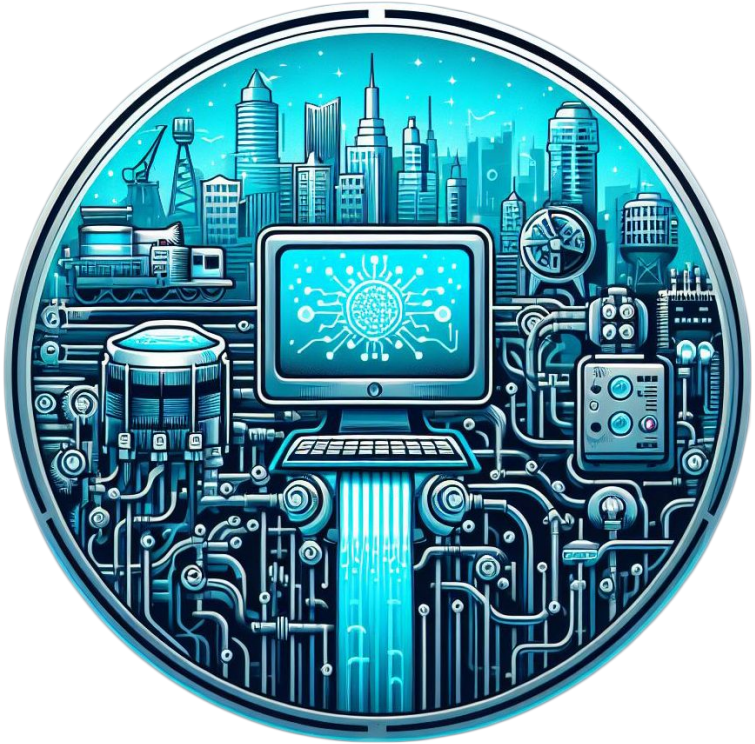
- Signup to Join the League Open: https://neccdl.org/neccdl/join
- Roster Submission Open: https://www.surveymonkey.com/r/2024CCDC
  - League Member Institutions will be provided information on Team Roster Submission **through Nationals**
- Jan 19, 2024:
  - NECCDC 2024 Registration & Roster Submission Deadlines (earlier registered = earlier access)
  - Public Resource (GitHub) Freeze Deadline: https://forms.gle/wF5FRbN1svFvNicS9
  - NECCDC 2024 Moderator Submission Deadline: https://forms.gle/vdpQUuMKgoZuRjda7
- Jan 27, 2024: Qualifier Beta Test (optional)
- Feb 03, 2024: NECCDC 2024 Qualifier
- TBD Feb 2024: Quals Outbrief & Regional Overview
- Mar 23-25, 2024: NECCDC 2024 Regional Onsite: 1 Pace Plaza, New York, NY
  - 10 Teams who qualify will compete for who will advance to Nationals
  - League Member Institution Delegates (Coaches) will meet to discuss future NECCDL topics

NECCDC 2024 Qual Schedule - Sat Feb 3, 2024

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 team channels.
14:30	Competition Ends	Blue Team access to environment systems will be disabled.

NECCDC 2024 Resources

- See our website for resources:
  - https://neccdl.org/neccdc/2024/resources/
- New or returning team orientation
  - Focused on new team orientation for Qualifier prep
  - Conducted by UBuffalo Coach: Dave Murray
  - Offered to registered League members
  - Reach out to orientation@neccdl.org if interested



CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

NECCDC 2024 Sponsors - Thanks for your support!

NECCDC 2024 Current Sponsors

U.S. National Science Foundation

Raytheon Technologies

PACE UNIVERSITY

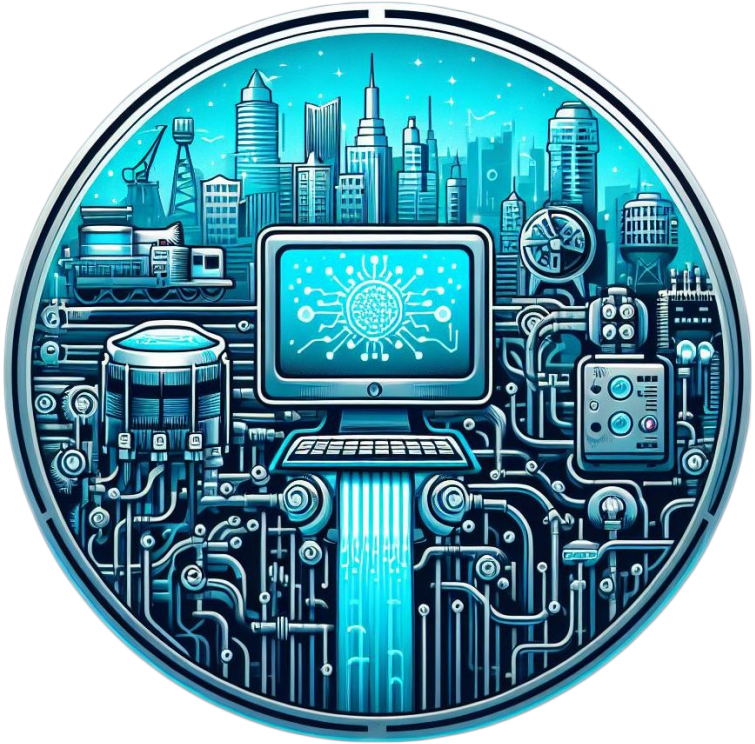
PACE UNIVERSITY

Seidenberg School of Computer Science and Information Systems

paloalto NETWORKS

Cybersecurity Academy

RSM



CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

Q&A