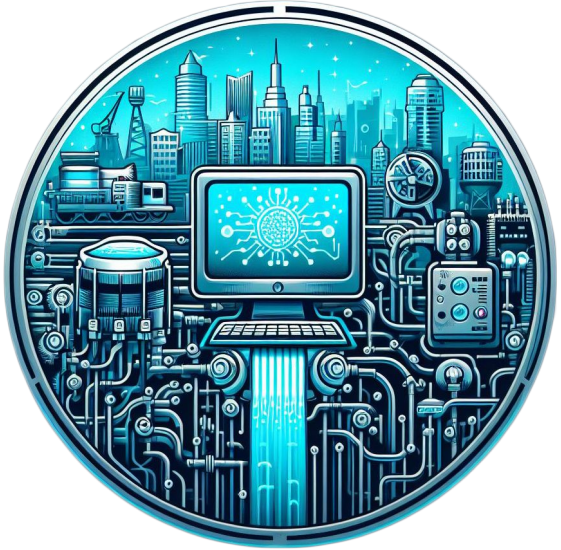
# NORTHEAST COLLEGIATE CYBER DEFENSE COMPETITION (NECCDC) 2024



CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

***Regional: Mar 23 – 25 2024***

*Hosted by*

PACE UNIVERSITY

*In Coordination with*

NECCDL

*In Partnership with*

NSF

Raytheon
An RTX Business

# Good Morning Competitors, Alternates & Coaches!

CHAMPLAIN COLLEGE

Northeastern University

RIT
Rochester Institute of Technology

UMASS LOWELL

PACE UNIVERSITY

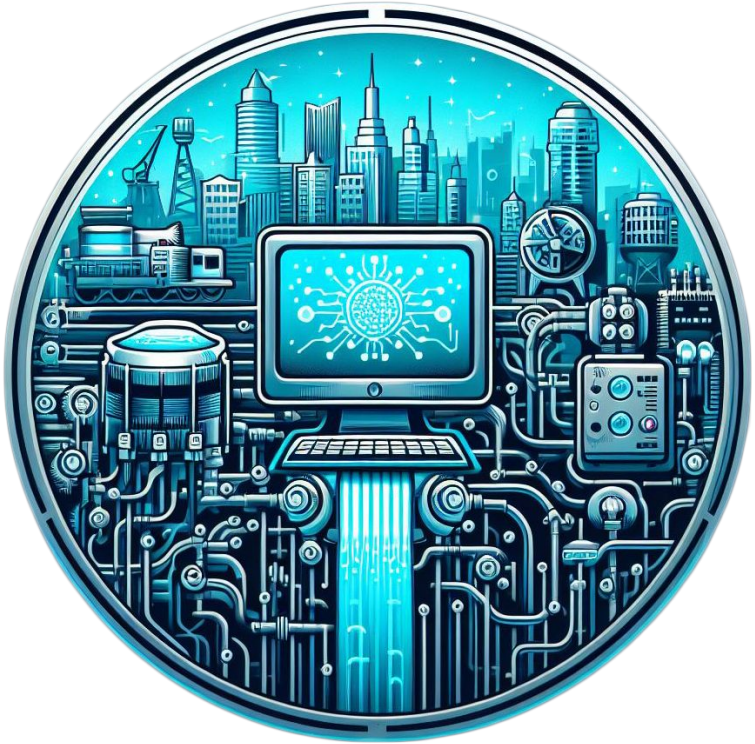
1865 THE UNIVERSITY OF MAINE

UMass Amherst

Syracuse University

Roger Williams University

UNIVERSITY OF NEW HAVEN
1920
CONNECTICUT



CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

# NECCDC 2024 Sponsors - Thanks for your support!

# NECCDC 2024 Current Sponsors


U.S. National Science Foundation

Raytheon
An RTX Business

PACE UNIVERSITY

Seidenberg School of Computer Science and Information Systems

PACE UNIVERSITY

Networking Academy
cisco

paloalto NETWORKS

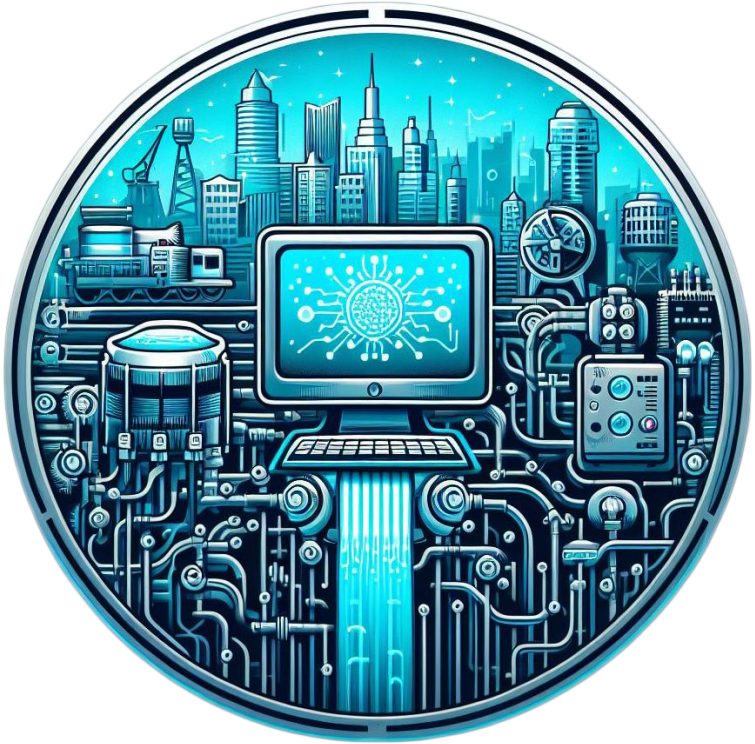


CROWDSTRIKE

FORTRA

BATTELLE
It can be done

RSM

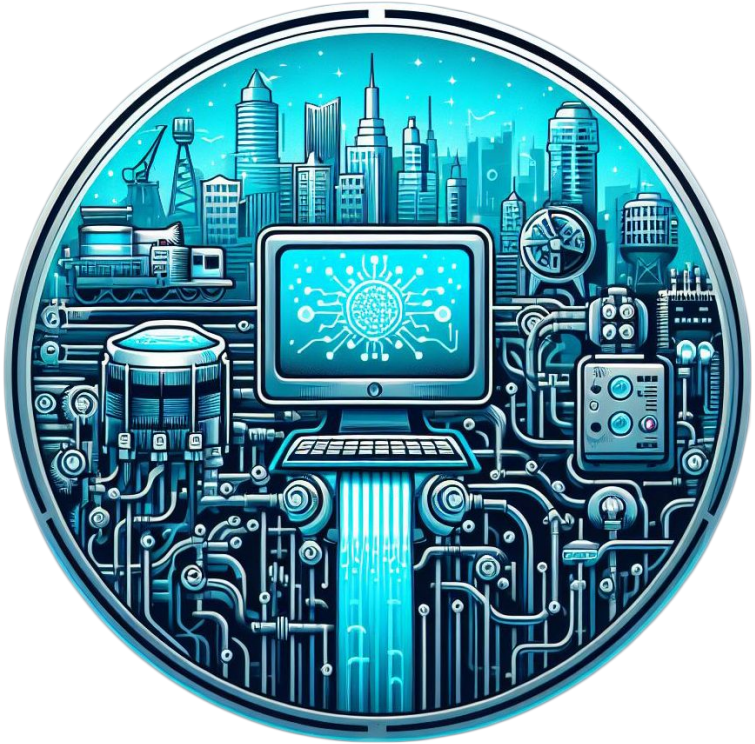


CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

# NECCDC 2024 Event Schedule

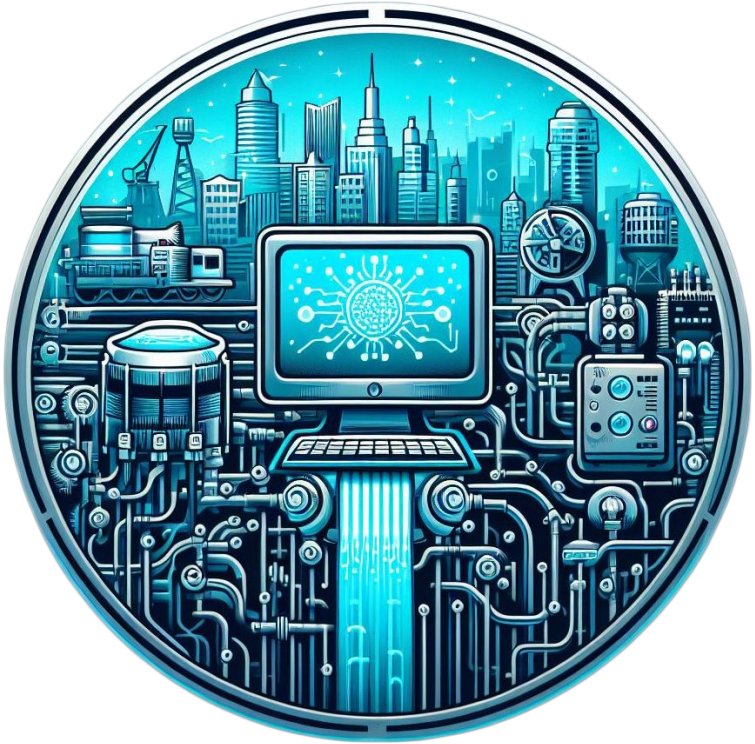
# NECCDC 2024 Event Schedule - Mon 3/25 - Day 3

| Start | End | Activity | Location |
|---|---|---|---|
| 8:30 AM | 9:30 AM | Breakfast (informal breakout) | Student Center, Welcome Center |
| 9:30 AM | 10:00 AM | Keynotes | Student Center, Welcome Center |
| 10:00 AM | 10:40 AM | Panel Discussions | Student Center, Welcome Center |
| 10:45 AM | 12:30 PM | Debrief & Awards | Student Center, Welcome Center |
| 12:30 PM | 2:30 PM | Lunch, Career Networking, Peer Networking | Student Center, Welcome Center |



CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

# *Please save all questions for the Q&A*

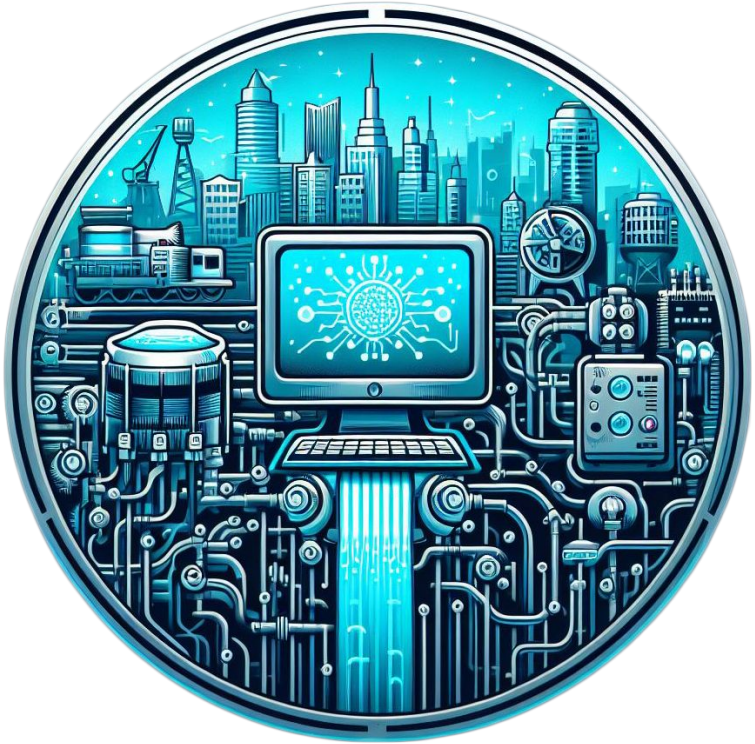


CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

# NECCDC 2024 Black Team Feedback

# NECCDC Black Team

- New Systems
  - Technology is moving faster than ever
- Identity Management
- Orchestration / Containerization
  - Audit what you have
  - Authentication
  - Configuration
- Assume Compromised
- Troubleshooting



CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

# NECCDC 2024 White Team Feedback

# NECCDC 2024 White Team Feedback - General

- ***RTFQ! Please!!!***
- Follow the format of the welcome inject for inject document naming
- Legitimate users need to be able to use their accounts
- Please don't upload files to VirusTotal - use free version hash comparison
- Executive Summaries should *summarize key points* in language that *executives* will understand
- Don't depend on To Do list in Google Classroom for all injects
- Provide evidence & submit on time!
- Mods can look young, but aren't blue team :) - ask them for requests to NECCDC officials

# NECCDC 2024 White Team Inject Review

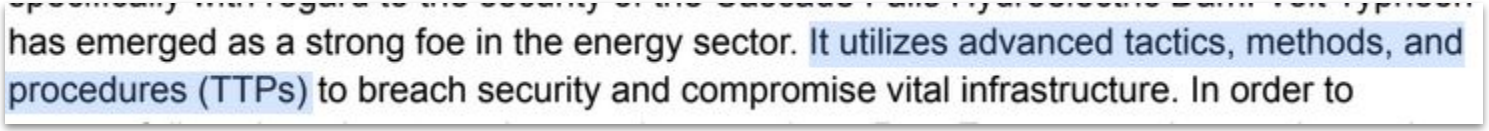
| Inject Title | Average Points Earned |
|---|---|
| Preliminary Assessment | 34%, 10/10 |
| Kubernetes Log Visibility and Compliance | 18.3%, 9/10 |
| Backups | 73.8%, 10/10 |
| Centralized Kubernetes Audit Logs | 21.8%, 8/10 |
| Backups Cost Money | 24% |
| Password Policy | 48%, 10/10 |
| Securing Kubernetes Application | 26%, 8/10 |

# NECCDC 2024 White Team Inject Review

| Inject Title | Average Points Earned |
|---|---|
| IT-OT Boundary Restrictions - Firewall | 44.4%, 10/10 |
| IT-OT Boundary Restrictions - Network Policies | 27%, 10/10 |
| External Audit User - Part 1 | 40.6%, 9/10 |
| Kubernetes Cluster Upgrade | 40.5%, 10/10 |
| External Audit User - Part 2 | 46.6%, 10/10 |
| External Audit User - Part 3 | 23.4%, 10/10 |
| Media Outreach Fact Sheet | 55.5%, 9/10 |

# NECCDC 2024 White Team Inject Review

| Inject Title | Average Points Earned |
|---|---|
| GitOps Deployment | 47.3%, 10/10 |
| ADCS Certificate Enrollment | 24.4%, 10/10 |
| Threat Actor | 55.2%, 10/10 |
| Create an Emergency Patching Policy | 34%, 10/10 |
| Exit Survey | 81.3%, 9/10 |



# NECCDC 2024 White Team News Reporter Inject

- Please do not talk about incidents to the press if you're not authorized
  - Don't lie to the press, that'll come back to bite ya later
- If you have a sign-in sheet, check what's being written
- No pictures in restricted areas!
- Few barriers to entry
  - Reporter likely saw confidential information
- Know what your company does please
- No one let us plug in the USB!!!
  - Or check her email

# NECCDC 2024 White Team Moderator Highlights

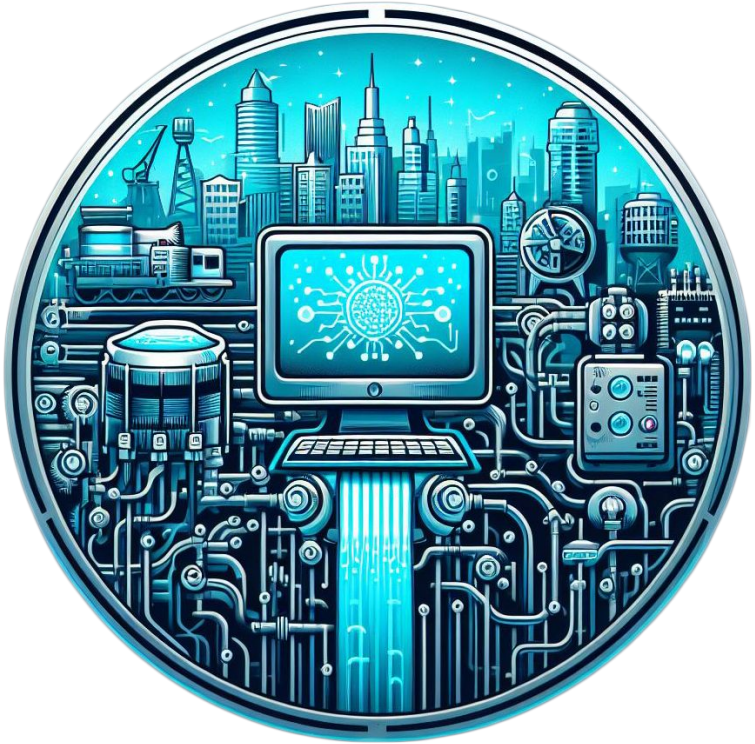
- Teams were all viewed as professional - calm & driven, communicative, cordial, respectful, sense-of-humor :)
- Standouts were those who:
  - had clear roles & responsibilities
  - had strong leadership who delegated / managed tasks
  - checked in regularly about deadlines & deliverables
  - thought ahead
  - came together when hitting roadblocks
  - used tools effectively, e.g., post-its, whiteboards, electronic communication
  - had experience troubleshooting & problem-solving
  - used AI / Google searches effectively (e.g., for troubleshooting errors, short scripts)
  - evaluated risk / reward of various options in decision-making
  - reached out to the correct communication channels

# NECCDC 2024 White Team Moderator Highlights

- Recommendations
  - Investigate updated commands - ifconfig may not be best command depending on UNIX
  - Use sed/awk and other command line utilities to filter results
  - Understand the software that you are using
  - Learn to break down problems into smaller ones to solve
  - Communicate with everyone - not just have 1-2 people talking
  - Learn to be receptive to all opinions & accept constructive criticism gracefully
  - Try to cross-train, don’t have a single point-of-failure / dependence on a single individual
  - Don’t let challenges bring you down - analyze, figure out possible solutions & move forward
  - Reach out for assistance earlier
  - Make sure you double-check bringing everything that you need :)
  - Focus on incident response - quick identification & remediation
  - Ensure there is a clearly defined leader
  - Celebrate wins!

CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

# NECCDC 2024 Red Team Feedback



CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

# Q&A