U.S. DEPARTMENT OF ENERGY'S
CYBERFORCE COMPETITION®
DEFENDING U.S. ENERGY INFRASTRUCTURE

NORTHEASTERN UNIVERSITY

NUCCDC

November 15, 2025

In-Person

Number of Teams	Max Team Points Received	Min Team Points Received	Mean Team Points Received	Total Points Possible
93	8,783	1,267	6,146.81	10,000

TEAM 63 SCORECARD

This table highlights the *team's* efforts for the 2025 CyberForce Competition®.

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	525	35.00%	28
Security Documentation	1078	86.24%	43
C-Suite Panel	785	62.80%	88
Red Team	875	35.00%	44
Blue Team	1603	80.15%	59
Green Team Surveys	1419	94.60%	52
Deductions	0		
Overall	**6285**	**62.85%**	**52**

ANOMALY SCORING

Anomalies simulate the real-world challenges that cybersecurity professionals face daily in the industry. These carefully crafted challenges not only test technical skills but also emphasize daily time management skills that professionals must demonstrate to effectively perform their roles. This year, challenges were longer, and some required more than one person to answer, effectively requiring teams to evaluate risk versus reward.

Anomaly Score	525

Below highlights whether the anomaly was correct or incorrect for your team.

1	Yes
2	
3	
4	Yes
5	Yes
6	
7	
8	No
9	
10.1	Yes
10.2	Yes
10.3	Yes
10.4	Yes
10.5	Yes
10.6	No
10.7	Yes
10.8	Yes
10.9	
11.1	Yes
11.2	Yes
11.3	Yes
11.4	
11.5	
11.6	
11.7	
12	
13	
14	
15	Yes
16	Yes
17	Yes
18	Yes
19	Yes
20	Yes
21	
22	
23	
24	
25	
26	
27.1	Yes
27.2	Yes
28	Yes
29	
30	Yes

ORANGE TEAM

Security Documentation

Blue team participants should use the Security Documentation section as an opportunity to highlight unique approaches to securing their infrastructure.

Security Documentation Score	1078

Strong Points	*Areas of Improvement*
• Good list of asset inventory and vulnerabilities. • The team demonstrated two key strengths: their network diagram was exemplary, clearly depicting all six systems, the subnet, and internet routing with effective labeling that aids leadership's situational awareness. Additionally, their vulnerability section was outstanding, documenting dozens of host-specific issues and mitigations far exceeding requirements, while successfully maintaining a concise,	• The overview was lacking, and too much jargon was used for addressing senior leadership. • The team needs to revise the document to achieve a top score. First, make the System Overview truly executive-ready by removing technical jargon like port numbers and using plain business language. Second, ensure the Asset Inventory is perfectly consistent with all other sections by listing every single service mentioned (like Modbus 502). Third, replace the weak Active Directory hardening (which allows RC4) with

Strong Points	*Areas of Improvement*
leadership-focused summary instead of raw tool output. - The hardening section shows deep technical understanding and strong application of layered security, logging, and monitoring. - Overall good documentation and easy to read. - Everything.	modern, best-practice Kerberos and NTLM policies. Fourth, use the exact, official VM names (e.g., "Public DB," "Task Box") consistently throughout the entire report and diagram. Finally, for the "assume breach" systems, add immediate compensating controls instead of just listing future actions, showing leadership how the risk is being managed now. - The vulnerability section could briefly group findings by system type or priority to make it easier for leadership to see the most critical risks first. - Remember that when you perform your system hardening you need to have concrete reasons for why each hardening step was taken. Someone with technical knowledge may know why but that is not always who will be reading the steps taken. - I really don't know; maybe more attention at minor details that could become major.

C-Suite Panel

C-Suite Panel will be a pre-recorded video based on the task outlined in this document. This video should be recorded and placed somewhere accessible to judges.

C-Suite Panel Score	785

Strong Points	*Areas of Improvement*
- You are headed in the right direction. Thank you for competing, - Good work including annual costs summary. - Well designed slides. - I really liked the schedule provided. The visual timeline was not required, but would speak to leadership. - Great quality video, clean professional briefing, and well balanced presentation skills. - Good introduction and professional. The high priority recommendations were realistic and you mostly explained how they would reduce risk. - Structure of the presentation provides a fairly good overview of the ICS compromise and the visuals are easy to follow.	- I could barely read the visual aids. Little to no eye contact with the camera. More thought was needed between the risks and the strategies. - Include more specifics on work completed by the other team members. - Quantify risks financially. How costly are the repairs? - Strategy include acronyms, these should be spelled out. - More details on the slide would help the viewer to comprehend and remember the recommendations. - A slide of referenced software and hardware could be included. - Could include costs to remediate. - For some reason the volume was very low. Perhaps on person mics would help? While the digital strategy was strong, i would have

Strong Points	*Areas of Improvement*
	liked to see a stronger holistic business strategy. • More visuals depicting actual data or solutions, tables or charts, would have enhanced your presentation. • There needs to be more thorough explanation about each risk and how they affect the bottom line. The risk reduction strategy should address those aforementioned risks as well. • No mention on how to improve and updated and improved HMI terminals and where log data could possibly be stored. If you can tie in similar real life cyber events, your high priority recommendations could be explained more seamlessly.

RED TEAM SCORING

Red Team Flag Inputs (Assume Breach & Whack a Mole)

This year we will be using ***Assume Breach*** as part of your Red team score. This will be worth *1,750 points*. The purpose of the assume breach model is for your team to investigate and accurately report back incident details after experiencing a successful execution of an attack chain. The **Whack a Mole** portion of the Red team score will be worth *750 points*. This will be done in a traditional method of "hacking" through holes created through known vulnerabilities in the system.

Assume Breach						
AB1	AB2	AB3	AB4	AB5	AB6	AB7
0	0	250	0	250	0	125

Whack a Mole		
WAM1	WAM2	WAM3
0	125	125

BLUE TEAM SCORE

The Blue team scoring (service scans) is completely based on the Blue team's ability to keep services active. In an industry environment, every security professional's primary responsibility is to keep business operational and secure. Service uptime is based on the required services and their respective uptimes. Teams earn points for each availability scan that results in positive service uptime for a total of 2000 points. Throughout the day, services will be validated as operational by the scoreboard polling system. Each service is scored and weighted the same, which means availability is scored purely on the service being operational.

Service Scans	ICS Score
1370	233

Each team was scanned *27 times* throughout the competition. Below identifies your team's number of successful service scans per required service. Each successful scan was awarded 5 points.

SMTP	IMAP	SMB (task)	NFS	SSH	HTTP	WinRM	LDAP	MariaDB	phpmyadmin	SMB (db)
27	27	27	27	27	27	11	22	27	25	27

The ICS Score was determined by the number of barrels you were able to produce during the competition. The max number of barrels a team should be able to produce (+/- slight variance) was 45,000 barrels. There were two periods in which minimal barrels, if any, should have been produced due to significant weather. The total number of points awarded was 515.

No. of Barrels Produced	Percentage of Total Barrels
20361.20	45.25%

GREEN TEAM SCORE

The Green team will review and complete surveys to evaluate each Blue team system's usability and user experience. Points will be awarded based on the user's ability to complete the tasks outlined in the user acceptance testing guide at the end of this document. The Green team will assess their ability to validate these tasks. The guide that will be provided to Green team users is available in the Rubrics section. It is in your best interest to run through this user testing to ensure that you can complete all the steps they are.

Green Team Score
1419

Green Team Survey Comments
• No footer on the home page. • The footer is not on every page, and the logos do not appear on the navigation bar on the admin page. • footer not showing in main page, logos in header doesn't show in user management page • footer not visible on main page • Recommend adding footer to the home page and watch the logo are not working on your member pages • Could not scroll to the bottom of the main homepage to validate the text at the bottom. Good luck! • you don't have a footer on the front page! otherwise, only a very small detail, but on the admin page the header logos do not load. • Suggest adding footer to home page like the others and watch your logos when login as Admin they get lost • Hello Team 63 footer text was missing on the main page. • Address footer is supposed to be on every web page, but it's not found on the home.