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

UNIVERSITY OF NORTHERN IOWA

UNI WOMEN'S RUGBY

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 92 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	457	30.47%	42
Security Documentation	1007	80.56%	58
C-Suite Panel	921	73.68%	67
Red Team	1125	45.00%	35
Blue Team	1769	88.45%	44
Green Team Surveys	1303	86.87%	44
Deductions	0		
Overall	**6582**	**65.82%**	**44**

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	457

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

1	Yes	10.7	No	17	Yes
2		10.8	Yes	18	Yes
3		10.9		19	Yes
4		11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6		11.3	Yes	22	
7		11.4	Yes	23	
8		11.5	Yes	24	
9		11.6	Yes	25	
10.1	Yes	11.7	Yes	26	
10.2	Yes	12		27.1	Yes
10.3	Yes	13		27.2	Yes
10.4	Yes	14		28	No
10.5	Yes	15	Yes	29	
10.6	Yes	16	Yes	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	1007

Strong Points	*Areas of Improvement*
• Has solid technical baseline, all six hosts are inventoried, the network diagram and vulnerability list are clear and actionable • Covered great amount of details with clarity and looking good to present. Overall great effort by the team. • System overview nicely defines what the assets do, which helps the c-suite better understand what it is they are reading about. All acronyms were spelled out prior to introduction, making this easier for the reader to follow. Diagram was professionally drafted.	• It could be expanded for ICS coverage and executive framing, add vulnerabilities/mitigations for the HMI and PLC, and update the System Overview and hardening sections. • More information can be added in system hardening section. • Include what the system does for the business as a whole and what the impact of the breach has been thus far. List assume breach devices in asset inventory. Need to identify switch/router in the network diagram. Further explanation of the

Strong Points	Areas of Improvement
• Good job on the overall document and being concise with the asset inventory. • The graphics used for the network diagram stood out.	processes taken in the system hardening, as well as describing the function of each tool would make this section more c-suite friendly. • The system hardening had a great start but needed to expand more on the why each step was taken and to be more elaborate than scan for vulnerabilities and patch. • Listing all the services in the asset inventory would have led to a more complete report.

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	921

Strong Points	Areas of Improvement
• Exceptional integration of quantitative evidence and operational realism. Approach was strategic, risk-aware, and actionable. • All team participated in the video. Multiple topics were discussed. • I love the that you able to show the graph and align them with the facts • Business and operation risks summary • Good job quantifying impacts to incidents. • You justified your long term strategy as well as your high priority actions. • I really enjoyed the technical translation very detailed, well explained!	• Video was too long. Could benefit from concise summaries tailored to C-suite. • Just over 7 mins, keeping it near 5 would have helped. • Risks were not clearly explained and analyzed (separately), time used was over 7 minutes, strategy and recommendations were difficult to follow and relate to the previous risks identified. • Be more specific on the improvement of the financial impact of the company • Emphasize future risks if strategy not implemented and high level strategy summary • Video is too long. Be concise and stick to around 5 minutes. You listed impacts of incidents, but not address likelihood, which is the other factor in risk. • How does your long term risk mitigation plan reduce the risks you specified? Your long term plan addresses how to prevent the current incident from happening again, but how do they reduce the overall risks you specify? • How much will your short term high priority actions cost? • The video was seven minutes long, consider trimming any excess information. For instance, on the “Risks and Concerns” slide, you discussed mitigations instead of focusing solely on risks. Since you later

Strong Points	*Areas of Improvement*
	have a dedicated “Mitigations” slide, you can keep those details there to make the flow more concise and clear.

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
125	125	125	125	125	0	0

Whack a Mole		
WAM1	WAM2	WAM3
250	0	250

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
1475	294

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	26	27	26	27	27	27	27	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
25750.79	57.22%

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
1303

Green Team Survey Comments
• there's no User Management' button .
• "Interesting Benefits on Careers page :-D But, Open Positions are all correct, so credit for this page. No footer on Home Page. Is this by design? It does not meet the criteria for site loading."
• Footer does not show on main page
• Good job!
• Excellent work!
• No footer on the home page
• The homepage does not have a footer.
• The homepage does not have a footer. The logos are not in the required positions.
• no footer on main page
• Could not scroll to the bottom of the homepage to validate the text. Good luck!
• footer not available on main page, logos flipped around
• Good work! All intended areas are still accounted for within the website and no issues locating anything per the requirements. I will say the logos in the header should be flipped according to the reference material that we were given.
• site cannot be reached
• This site can't be reachedweb.blue0092.cfc.local refused to connect.