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

THE UNIVERSITY OF RHODE ISLAND

RHODY RAMS

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 2 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	386	25.73%	59
Security Documentation	1007	80.56%	58
C-Suite Panel	936	74.88%	65
Red Team	625	25.00%	67
Blue Team	1619	80.95%	56
Green Team Surveys	1031	68.73%	65
Deductions	0		
Overall	**5604**	**56.04%**	**65**

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	386

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

1	No
2	
3	
4	
5	Yes
6	
7	
8	
9	No
10.1	Yes
10.2	Yes
10.3	
10.4	
10.5	
10.6	
10.7	
10.8	
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	No
29	No
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*
• Great network diagram and overall approach to the document. • Good network diagram and hardening steps. • Excellent documentation. Reads like something you'd hand to management. • Overall the security documentation was thorough and covered the requirements.	• Ensure that you follow word count limits, such as in the system overview section, which also could have been more high level (this would have brought word count down). Also, some finer details could have been improved such as using no italics/consistent font sizes on the vulnerabilities section and in the system hardening section, either using full sentences or turning the fragments into some bullet points for readability.

Strong Points	Areas of Improvement
	• Some jargon was used in the overview, which should be avoided for senior leadership. • Could tighten writing a bit. Some sentences run long and repeat details. • A few changes could improve this security documentation, specifically the System Overview could have a more holistic view which identifies the purpose with respect to the organization. The HMI and PLC boxes should have their Known Vulnerabilities identified, but not mitigated.

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	936

Strong Points	Areas of Improvement
• Excellent Timeline and Business Impact slides. • Clearly connected business impact/risks to the security risks. Recommendations are clear and appropriate with reasoning. Professional presentation . • High-priority recommendations were solid (although there was some confusion regarding what constitutes "a SCADA") • All presenters spoke clearly and in a professional manner. Great work so far! • The presentation was clear and concise. • Sharing the relevant information, and keeping the audience attention focused on your explanation. • Clean, professional, and consistent presentation visuals. Very well polished presentation.	• Be enthusiastic about your subject. Speak loudly, possibly consider standing for the presentation to allow more air in your lungs. When giving dollar amounts (B - billions, M - millions, K - thousands) to avoid lots of zeros. Add "$" in front of financial amounts (Business Impact slide). Capitalize application names so they stand out from the other words on slides (Hi Pri Recs slides). Still had 30 seconds to share YOUR EXPERTISE!!! • Business impact is not strategy to reducing risk and even a minimal discussion of a strategy to reduce risks would have been helpful. The length of 4.5 minutes does not match with missing an entire element of the presentation (strategy) • Acknowledged risks and tactical, high-priority recommendations, but provided no long-term, strategic risk-reduction strategies. • Findings timeline would be easier to follow if it was one straight line. For future timelines, consider placing information above and below the line so it fits in one line. SCADA should be spelled out on first use for those who are not familiar. It is important to remember, while a tool may be free, there is still funding needed for staff to complete

Strong Points	*Areas of Improvement*
	the work or to set up the standard operating procedures before a tool can be used (e.g., FreeFileSync) • Students should present more freely, be more confident in what they say, and the team should be more united. • With impactful and active interaction. • Presentation felt organic but try to avoid use of filler words ("um"). Risks were clearly tied to financial operations and reputational damage. Risks and recommendations are provided, but the strategic plan should be stronger. Emphasize strategic risk mitigation and this becomes an exemplary presentation.

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	125	0	0	0	0	0

Whack a Mole		
WAM1	WAM2	WAM3
250	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
1200	419

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)
8	7	27	25	24	24	27	27	27	17	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
36683.98	81.52%

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
1031

Green Team Survey Comments
• Page does not load • Fails to load • blue admin got deleted. green user deleted • For the one segment marked as False 'Check admin users are listed' - the users 'blue@obsidianrift.oil' and 'green-admin@obsidianrift.oil' were not on the list itself, the general 'users' were. • When in as admin do not see the blue or green admin user - also probably want to fix the footer so it appears on home screen, it is on the others. • admin users not visible. Footer text missing on homepage. • Homepage needs a header. Admin page is missing green & blue admins • Site looks good, but I had no access to the 'Admin Dashboard'. I could log in and there was no 'Admin' button, but it only returned me to the main screen. • The footer is not on every page, and there are no admins listed on the admin page. • "No Footer on Home Page. Logging in as normal user takes me right to user admin page. And Admin button shows. Not all users show up when admin logged in." • no users found in user management, footer not available on main page • both users have Admin button. cannot access the page with all of the users. • Your login pages are not working, general user is seeing Admin button and when logged in as Admin don't see any users. The logos are in the wrong spot and the footer isn't on the home page.

Green Team Survey Comments
• Logins not proper, non admin see admin link, admin see no users, logo in wrong spot and footer not on every page • Site is down • This site cant be reachedweb.blue0002.cfc.local refused to connect. Try: Checking the connection; Checking the proxy and the firewall; ERR_CONNECTION_REFUSED"