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

RADFORD UNIVERSITY

RUSECURE?

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 75 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	411	27.40%	53
Security Documentation	1066	85.28%	48
C-Suite Panel	886	70.88%	76
Red Team	875	35.00%	44
Blue Team	1661	83.05%	55
Green Team Surveys	1369	91.27%	53
Deductions	0		
Overall	**6268**	**62.68%**	**53**

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	411

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

1	No	10.7	Yes	17	Yes
2		10.8	Yes	18	Yes
3		10.9		19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6		11.3	Yes	22	
7		11.4		23	
8		11.5		24	
9		11.6		25	No
10.1	Yes	11.7		26	
10.2	Yes	12		27.1	
10.3	Yes	13	No	27.2	
10.4	Yes	14		28	
10.5	Yes	15	Yes	29	
10.6	No	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	1066

Strong Points	*Areas of Improvement*
• Overall well great work! Asset inventory and system hardening systems sections were well done. • I like the creative diagram and detail documentation • The hardening steps were comprehensive and well thought out. • The system hardening is well thought out and explains the process in detail. Great job providing the term before introducing the acronyms.	• The known vulnerabilities section can be improved for senior leadership by using appropriate language for better understanding and decision-making. • The asset inventory was missing ports and services. • Speak to recent breach in system overview. Task missing port 25. PLC missing port 502. Network diagram missing switch/router. • Even if you can't mitigate vulnerabilities on the HMI and PLC systems, their vulnerabilities should be enumerated. System hardening portion was hard to

Strong Points	Areas of Improvement
• Summarized/grouped several vulnerabilities caused by outdated software, instead of individual entries for each.	follow, and intermingled enumeration and remediation steps with hardening steps.

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	886

Strong Points	Areas of Improvement
• I like that you wanted to create an incident response and disaster recovery plan. • Good work including sources. Include work completed or work roles of the other team members. • Good quantifying the risk • Clearly outlined business risks and operational impact following an industrial control system compromise, with direct ties to reputation, safety, and production. • Very good job at quantifying the impacts for risk. I love that business continuity is listed as a high level strategy. You did a great job providing cost estimates when possible. • Long term actions looked logically sound.	• expand on the summary. Don't just read your slides. If you mention creating an incident response and disaster recovery plan, provide more details about it. • For strategies include timelines, costs, software and hardware requirements, and training requirements. • Recommendations could be more quantified (financial analysis of prevention costs versus risks) and tailored to Obsidian Rift Energy's specific environment. Vendor management and risks were not highlighted. • Your listed risks are largely just impacts, which is only one part of the equation for risk. How do your strategies reduce your listed risks? For your high priority actions, you say costs will be "minimal" because you'll be using internal staff. Internal staff aren't free. About how many hours of labor are we talking here? Just because internal staff are getting paid anyways, does not mean there is a cost. Every hour you spend on your cybersecurity actions is an hour you are not spending somewhere else. • Some slides were suitable only for some members of the C-suite. Real-world feasibility of high priority recommendations with open source tools is difficult.

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	0	0	125	0	0	0

Whack a Mole		
WAM1	WAM2	WAM3
125	250	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	186

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
16285.65	36.19%

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
1369

Green Team Survey Comments
• Great job, good luck! • red user created, • You're doing great! • Check your site . . . the image and tag has been replaced! • This site can’t be reached web.blue0075.cfc.local refused to connect. • 5:53 This site can’t be reached