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

AUBURN UNIVERSITY

THE BEARS

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 84 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	435	29.00%	46
Security Documentation	1097	87.76%	40
C-Suite Panel	1044	83.52%	35
Red Team	1750	70.00%	8
Blue Team	1826	91.30%	33
Green Team Surveys	1079	71.93%	25
Deductions	0		
Overall	7231	72.31%	25

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	435

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

1	Yes	10.7		17	Yes
2		10.8		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	
10.1	No	11.7		26	
10.2	Yes	12		27.1	Yes
10.3	Yes	13		27.2	Yes
10.4		14		28	No
10.5		15		29	
10.6		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	1097

Strong Points	*Areas of Improvement*
• Good level of descriptions on most of the mitigations. • The hardening section shows excellent organization and thoughtful application of real-world cybersecurity practices. • Strong list of vulnerabilities, followed all formatting guidelines from rubric/template • The network diagram was labelled • The Network Diagram, the way they list the vulnerabilities and next steps of remediation. Also, the explanation of the threats	• System overview not written for CISO level. Missing ports on inventory. • Adding brief summaries or metrics at the start of major sections would help readers quickly see progress and outcomes. • Network diagram needs more detail (what are each of these assets?), asset inventory has some small mistakes • listing all the assets by host is a better way to go than having them listed scattered

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	1044

Strong Points	*Areas of Improvement*
• Both speakers were well spoken and have obviously rehearsed their parts. Slides were easy to understand. Good pacing. Refreshing presentation after 10 others. Lots of energy and expertise. • Your slides were easy to read. You didn't read off your slides. Your slides for risk reduction were well laid out and showed cost and timeline. • Covered and outlined business risks and operational impact following an industrial control system compromise, with direct ties to reputation, safety, and production. • Overall, this was a good presentation. The speakers spoke confidently and were thorough in their explanations of each topic area. • Good job attempting to cover all aspects of the security risks. • Great recommendations, well-rounded plan to improve cybersecurity	• Label speakers under their videos. Current Impact slide - skipped over 3rd set of bullets. Top Priority slide - add costs and time needed. Next Steps slide - provide time needed for each step. Risk Reduction slide - speaker covers up 2 bullets. Timeline is really time needed - a timeline shows all steps on the same graph. Last summary slide was a bit confusing - you controls what the graph looks like; recommend upward sloping/small risk to big risk with a TOTAL COST shown. "Thank you" - should be "Questions" • Could have been more professionally dressed and your language was very casual. • Vendor management could be more specific. • The costs associated with high priority were higher than expected. I recommend exploring more low cost/no cost application options. In terms of presenting, take your time, and talk a little slower to help the audience follow along. If you are sitting in a chair with wheels or that leans back, try to sit still to keep distractions to a minimum. • Focus more on what the target audience will want to hear and be precise about it. • The two presenters were great, but I would have loved to hear more about how everyone else on the team contributed to your briefing. It was great to see such passion about how to improve the security posture, but at times it felt more appropriate for an infomercial or YouTube recording, not so much something for C-suite.

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
250	250	125	250	125	0	250

Whack a Mole		
WAM1	WAM2	WAM3
125	125	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
1425	401

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	20	27	27	22	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
35058.05	77.91%

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
1079

Green Team Survey Comments
• Make sure you are using the proper color accents and your footer is missing • The footer is not on every page. • Background image is low and under it another image is upside down • No footer on the home page • there's no manage button when log in. • No footer on home page • footer not showing up on main page, additional users, • Could not validate the text at the bottom of the homepage. Good luck! • Address footer is supposed to be on every web page, but it's not found on the home. • Hello Team 84. The footer text was incorrect it states Redrum Headquarters and not ObsidianRift Energy Co. Headquarters and the footer text was missing on the main page. The top navigation bar reads Hacked. • 5:08 This site can’t be reached • 5:33 504 Gateway Time-out • web.blue0084.cfc.local refused to connect. • website is down • web.blue0084.cfc.local refused to connect.