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

DRURY UNIVERSITY

D PANTHERS

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 35 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	229	15.27%	85
Security Documentation	714	57.12%	88
C-Suite Panel	583	46.64%	92
Red Team	125	5.00%	87
Blue Team	1300	65.00%	86
Green Team Surveys	469	31.27%	87
Deductions	0		
Overall	**3420**	**34.20%**	**87**

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	229

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

1	No
2	
3	
4	Yes
5	Yes
6	
7	
8	
9	No
10.1	
10.2	
10.3	
10.4	
10.5	
10.6	

10.7	
10.8	
10.9	
11.1	
11.2	
11.3	
11.4	
11.5	
11.6	
11.7	
12	
13	
14	
15	No
16	No

17	No
18	Yes
19	Yes
20	Yes
21	
22	
23	
24	
25	
26	
27.1	
27.2	
28	
29	
30	

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	714

Strong Points	*Areas of Improvement*
• Network diagram was solid, understandable, and detailed for reference. • The network diagram looked great • Covered good amount of details. • Great network diagram! • The network diagram is clear, easy to read, and has a legend.	• Sentence structure was a bit clunky throughout the system overview, which could have used a bit more explanation and detail. Service listings seemed off/missing components within the asset inventory. Not all vulnerabilities identified had corresponding mitigations listed. A more strategic approach to describing how system hardening was approached would have been beneficial instead of a completed to-do list. • Very little detail given in system overview. Vulnerabilities were lacking mitigations.

Strong Points	*Areas of Improvement*
	• There are lot of details missing from the assignment in the vulnerability section and some of the formatting can help. • The vulns, system overview and system hardening sections were a bit lacking. Would have liked to see some type of SIEM strategy. • Vulnerabilities could have been better researched and mitigation techniques should have been listed for each.

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	583

Strong Points	*Areas of Improvement*
• Thank you for competing. • The slides had clean graphics that were not distracting. • Recognizes key business and regulatory risks such as fines and safety issues. • Good overview of second-order business risks.	• The video and presentation was not professional. Risks and strategies needed to be worked out and the overall presentation needed to be reworked. • Risks were only addressed in isolation and not summarized as whole. No real strategies were given, but a broad overview of what the strategy should be. A broad discussion of recommendations was discussed, but there was no discussion of specific recommendations, and not tied back to the identified risks. Overall, a lot of time was spent on giving an overview of scenario when this time should have been allocated to specific risks, strategies, and clear action recommendations. • Explanations remain very surface-level; minimal evidence of structured mitigation or strategic thinking. Business risks slide with giant video and hand movement was jarring. • The team follows an appropriate dress code however there are minor visual distractions (excessive hand gestures and poor camera quality). Additionally the slide deck, perhaps, was out of order. In the Overview of Situation (slide 2) the presenter jumps straight into the overview of the incident. Then in the Business Risks (slide 3) the presenter introduces himself. Additionally, formatting across the slides is inconsistent and decreases the professionalism aspect

Strong Points	*Areas of Improvement*
	of the overall presentation. The presentation is the right length but only one other team member is acknowledged in the opening statements. • Lost data is lost data, if it is exfiltrated it cannot be recovered - this is not a good high priority item. Overall, the high priority items do not provide cybersecurity actions to improve the overall security posture of the system. They are focused on immediate recommendations to restore functionality and prevent a rig shutdown with a comment on maintaining physical safety for rig workers but offer no cybersecurity recommendations for security controls with longevity. Furthermore, the strategy simply states that the team will secure, regain, and control the system with no comment as to how or what tools they will use to implement this strategy. There is also no reference to how this strategy will support the company in the long term nor how this reduces risk overall. This presentation lacks a clearly defined, actionable list that C-suite executives could walk away and begin acting upon. • Lacks justifications and detail. Spent a lot of time describing the incident at a level not needed by the CISO. Video felt choppy, re-introduced a team member? • Recommendations and strategy did not directly relate to identified risks, and did not identify how they would improve the overall security posture.

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	0	0	0	0	0

Whack a Mole		
WAM1	WAM2	WAM3
0	125	0

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
1300	0

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)
20	20	25	26	26	18	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
0.00	0.00%

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
469

Green Team Survey Comments
• This site is compromised: color scheme is wrong, no Admin, no footer, no tagline, no logos.

Green Team Survey Comments

- Website needs a some work, many aspects were incorrect or missing. I could not log in to the 'Admin Dashboard', there was no 'Login' button. The careers on the 'Careers' page were incorrect. The header was also missing the logos.
- Wrong color page, missing footer on home page, should say 'ObsidianRift Energy Co.' in navigation bar, all career listings missing, no ability to log in, logos missing in navigation bar as well.
- Your site is not matching to all criteria, please check your accent colors, your missing the Login ability, your career page lists the positions and has the label in the form but no way to pick the position to apply for, no way to login, will say footer is there but check why not showing on home page, and logos are missing
- "Colors hacked. No footer on home page. No signin button. No Career positions. Logos gone. But, Rig Status is valid.
- Footer Text is missing 'Rift'.
- 404 not found
- Logo is missing for both ObsidianRift/Abyssal Pearl. No login for user/admin. Color wrong.
- Site is yellow and header is missing logos and login button; no careers listed
- Cannot log in, careers missing, website title should be 'ObsidianRift Energy Co.'
- logos is missing, footer is missing on the home page, career is missing those positions
- cant connect
- site cannot be reached
- This site cant be reachedweb.blue0035.cfc.local refused to connect.
- Site is down