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

BRIGHAM YOUNG UNIVERSITY

BYU CYBERIA

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 70 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	575	38.33%	22
Security Documentation	1070	85.60%	46
C-Suite Panel	973	77.84%	54
Red Team	1500	60.00%	14
Blue Team	1952	97.60%	8
Green Team Surveys	1123	74.87%	26
Deductions	0		
Overall	**7193**	**71.93%**	**26**

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	575

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

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

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

17	Yes
18	Yes
19	Yes
20	Yes
21	
22	
23	
24	No
25	
26	
27.1	Yes
27.2	Yes
28	Yes
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	1070

Strong Points	*Areas of Improvement*
• Good explanation of system, appropriate for executive audience • The report was simple but the content was solid. • Good job on ensuring a complete asset inventory and on identifying and mitigating quite a few of the vulnerabilities. • listed the asset inventory and their attributes. mentioned the incident response handling process taken, and also the team included the links in there in case anyone in leadership needed more details.	• Some vulnerability mitigations lacked justifications (user appears "out of line" with other users). Some listed vulnerabilities aren't really "vulnerabilities", per se (e.g. banners) • The formatting could have been clearer to delineate elements and highlight important parts. • Just because I know why you did each action to harden your system does not mean that there is any sufficient justification provided.

Strong Points	*Areas of Improvement*
	• For next time, ensure documentation presented to leadership is thorough without extra empty pages

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	973

Strong Points	*Areas of Improvement*
• The presentation overall was well done and well reasoned out. • The presentation is well-organized, covers all key risks and solutions, and provides actionable, cost-effective recommendations that are clearly linked to business priorities and resilience. Uses open-source tools effectively. • I like the detail information. • good teamwork between the presenters and well laid out slides. • Clearly outlined business risks and operational impact following an industrial control system compromise, with direct ties to reputation, safety, and production. • You do a great job prioritizing the actions that your recommend taking now, but probably too much of the talk is dedicated to that. Note that your cost estimate is way too low (you were not graded down for this, just FYI). Consider other costs, such as disruption, hours you'll need of non-cyber staff, etc.	• Strategies needed to be tied back to the risks and business concerns. Some slides had a lot of wording. Overall, well reasoned out. • Recommendations are somewhat generic and lack prioritization or linkage to specific risk outcomes. The presentation could be improved by quantifying financial impacts (e.g., estimated downtime costs) to give leadership a clearer sense of urgency and return on investment. • Needs to address the impact on finances of the company! • a bit too techy detail if not overly on the jargon • Recommendations could be more quantified (financial analysis of prevention costs versus risks) and tailored to Obsidian Rift Energy's specific environment. • You don't have a long term strategy for reducing risks? What are the longer term investments that will improve your security posture and lower the likelihood and impact of another attack?

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	0	250	125	0	0	250

Whack a Mole		
WAM1	WAM2	WAM3
250	250	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
1470	482

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	25	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
42153.10	93.67%

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
1123

Green Team Survey Comments
• Homepage says 'spilling oil is good'

Green Team Survey Comments
• Address footer is supposed to be on every web page but it is not found on the home.
• your site is down! returns a 500 error.
• Site completely broken, no access to anything.
• "Normal User: Admin available in header menu drop down with narrowed browser window. Able to get to Admin user management and demote blue admin which deleted the blue admin user. No footer on home page."
• No footer on the home page
• footer not available on main screen, Blue admin and green user not visible in user management
• blue@obsidianrift.oil is not listed under User Management, other than that it looks great!
• footer not available on main page, no blue admin on user management
• missing footer on homepage, the admin login functionality is missing account as admin
• No footer on a home, only 1 admin user.
• Good job the image is covered mostly though
• Perfect!
• green user missing in user management
• web.blue0070.cfc.local refused to connect.
• 5:53 This site can’t be reached