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

DEFENDING U.S. ENERGY INFRASTRUCTURE

CHICAGO STATE UNIVERSITY

CSU COUGARS

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 17 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	225	15.00%	86
Security Documentation	442	35.36%	92
C-Suite Panel	813	65.04%	87
Red Team	125	5.00%	87
Blue Team	1475	73.75%	68
Green Team Surveys	241	16.07%	89
Deductions	0		
Overall	**3321**	**33.21%**	**89**

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	225

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

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

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

17	No
18	Yes
19	No
20	Yes
21	
22	
23	
24	
25	
26	
27.1	No
27.2	No
28	No
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	442

Strong Points	*Areas of Improvement*
• The team made a good attempt as either new to the competition or didn't have enough time for a complete document, but still turned in what you could before the deadline. What you do have is a good start. • Organized and professional-looking. • Attempts were made to demonstrate security best practices • understand the environment and scenario	• Missing a lot of information, 2 out of 6 systems weren't found or documented, and detail lacking in every section. System Hardening section claims that a lot more was done than is apparently accomplished - honesty could have gained more points within Professionalism and Format category. • Feels too high-level. It needed more detail about what was actually done. • This documentation would benefit from closer attention to detail, greater technical depth, and more editing. Ensure that

Strong Points	*Areas of Improvement*
	information and recommendations provided align with the given scenario and rubric. - Focus on completeness and executive framing—make sure all six VMs and ICS pieces appear in every relevant section (inventory + diagram) and add a short, business-impact summary

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	813

Strong Points	*Areas of Improvement*
- Change contractor policies - few teams recommended this (good job). Great conclusion. - Good job sticking to the 5 minute limit and avoiding technical jargon. - It looks like you had some technical issues with your video. Good job getting the submission in. The length of time was good and all important topics were covered. - Outlined business risks and operational impact following an industrial control system compromise, with direct ties to reputation, safety, and production. - Presentation content was great and well spoken so that C-suite could mostly understand what was being discussed. - Risks were mentioned and some strategy to reduce the risks	- Two intros of team members were not the same. Videos obscured part of the text. Recommend using name labels under the videos. 2nd speaker should try to remain still while talking; recommend having another person in the room so that he can "have a conversation with them" and reduce any nervousness. Text runs over the right side of the screen. Estimate cost of 200,000 barrels to show $$$ cost to company. Green backlights were distracting for 2nd speaker. Would like to see the slide while the 2nd speaker is talking. - Slides were cut with how the video is recorded, e.g. I can only see ‘Presented by:” and “Abyssal Pearl P” in the first slide. Almost half of the priority slide was cut off. - It is unclear if all team members were acknowledged in the slide (if it was cutoff) or if the speakers presenting comprised the full team. If not, all should have been acknowledged. - The outlined strategy didn’t have enough detail. For instance, what specific environmental safeguards do you mean in the ‘Reduction Strategy’ slide? Furthermore, strategy was not tied enough to risks. - Cost of many items was not discussed sufficiently, which is something very important to the c-suite. For instance, reinforcing staff awareness costs money—how much? And what does this look like in practice—e.g., a training course? How much does ‘regular threat hunting’ cost?

Strong Points	*Areas of Improvement*
	• It would have been better to have had slides and just your voices in the background than only talking through the slides. • Recommendations could be more quantified (financial analysis of prevention costs versus risks) and tailored to Obsidian Rift Energy's specific environment. • Review your video before uploading or even after to make sure it uploaded properly. Would have given higher marks if the slides were not included and your team just spoke to the camera. • For the next presentation, it would be helpful to check the display settings. The sides of the slides appeared cut off; focusing on your delivery also could enhance audience engagement.

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	0	0	0	0

Whack a Mole		
WAM1	WAM2	WAM3
0	0	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
1430	45

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	18	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
3998.10	8.88%

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
241

Green Team Survey Comments
• Website needs a great deal of work, many aspects were incorrect or missing. • hacked while doing survey • Not properly landing on the page. • Can't scroll down homepage; may be Red Team. • Login credentials doesn't work nor does the rig status page. • color is inconsistent, name of company is wrong in header, company address is wrong in footer, could not login, no logos in header, image and tagline are wrong, no careers listed • Unable to load site • company name misspelled, unable to log in, footer messed up, rig status page errors out • Site is down