LEWIS UNIVERSITY

CYBER FLYERS

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 20 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	271	18.07%	79
Security Documentation	840	67.20%	79
C-Suite Panel	859	68.72%	82
Red Team	750	30.00%	53
Blue Team	1171	58.55%	89
Green Team Surveys	215	14.33%	84
Deductions	0		
Overall	**4106**	**41.06%**	**84**

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	271

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

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

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

17	Yes
18	Yes
19	Yes
20	No
21	
22	
23	
24	
25	
26	
27.1	No
27.2	
28	No
29	
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	840

Strong Points	*Areas of Improvement*
• Very good descriptions and the legends were particularly helpful • great structure, formatting, and organization • The report reads like real incident report, was appropriate for c suite, clear formatting. • Adding in an explanation in addition to the mitigation for the vulnerabilities was well done. • good list of asset inventory	• Consider adding a step in system hardening to allow for monitoring for future attacks, such as logging and alerts. • draw more connections in network diagram • Content was a bit light in the system hardening section. • Expand more on the system hardening, it had a really great start. • The hardening section seemed AI generated. It lists tools but not justification for using them.

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	859

Strong Points	*Areas of Improvement*
• Very professional slides and presentation quality • I enjoyed it was not death by slides. • In isolation the strategy and recommendation were good, however, it lacked a better correlation of risk-mitigation-recommendation. • Professional slides, and graphics. Presenters were professionally dressed. • Highlighted the effect of the attack on production, safety, and reputation, and the critical importance of direct communication with business stakeholders. • Very strong. • Explained how to fix and prevent the issue. • No jargon. • Defended the actions the team should take with reasons.	• Missing many components outlined in the rubric, i.e., too little detail for C suite. How does the strategy mitigate the operational and business risks? What is high priority and why? • You could have expanded on the risks and the strategies for the attack. • Better explanation of the risks, since overall is difficult to track the risks towards the strategy and recommendations. • Did not introduce other team members that were not on the recording, nor discuss their roles. • Risk should be quantified in monetary value when possible. This can be estimated. • For Mitigation Strategy and Recommendations include more specifics such as staffing, software, and hardware requirements, cost, and timelines. • When considering weekly backups is the organization willing to risk losing a week's worth of data? • The risks are mostly to ICS systems and related attacks, encryption may not be a priority at this time as the emphasis is not on protecting data, but hardware risks associated with intrusions. • It may be beneficial to include references and suggested software/hardware. • If reading a script it would be recommended to run through the presentation a few times to increase the comfort level. • Presentation could benefit from stronger technical recommendations (incident forensics, zero trust architectures). Recommendations could be more quantified (financial analysis of prevention costs versus risks) and tailored to Obsidian Rift Energy’s specific environment. • May want to use some numbers to quantify the value of not implementing these actions.

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	250	0	0	0	0

Whack a Mole		
WAM1	WAM2	WAM3
250	125	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
1160	11

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	26	27	0	27	25	18	21	27	7	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
1023.36	2.27%

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
215

Green Team Survey Comments
• Will not load website
• no logos in the header. no login button, no footer, no listed career pages.
• no login, oil rig picture changed, tagline different, rig page not loading
• site went down as i was doing survey
• not loading
• the landing page is not properly formatted and other links not working.
• unable to load site
• Missing all components.
• Hello Team 20. I was unable to log into the admin middleware , and the logos on the header were missing, the footer was missing on the main page. There were no career options to select from, the navigation bar did not include a log in option. The home tagline states that The Spilling Oil is Bad. Spilling Data is Better, it should be Spilling Data is Worse. And when going to rig-status page I receive this error: SQLSTATE[HY000] [2002] No such file or directory (Connection: mysql_historian, SQL: select * from `production`) Also the background image should have a photo banner with an Oil Rig.
• incorrect spelling in header, wrong background image and tagline, no available career options, no log in option, incorrect information in footer, cannot load rig-status page, no logos in header
• no logos, no login button, no footer on the homepage, oil rig status broken
• no login button, main page all scrambled, company name changed, footer changed, rig status page erroring,
• Site is down