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

LEWIS UNIVERSITY

ORDER OF THE PURPLE FLAMINGO

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 64 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	426	28.40%	49
Security Documentation	1150	92.00%	23
C-Suite Panel	1002	80.16%	47
Red Team	1500	60.00%	14
Blue Team	1974	98.70%	4
Green Team Surveys	1352	90.13%	14
Deductions	0		
Overall	**7404**	**74.04%**	**14**

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	426

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

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

10.7	
10.8	
10.9	
11.1	Yes
11.2	Yes
11.3	Yes
11.4	Yes
11.5	Yes
11.6	
11.7	Yes
12	
13	
14	
15	Yes
16	Yes

17	Yes
18	Yes
19	Yes
20	Yes
21	
22	
23	
24	
25	
26	
27.1	Yes
27.2	Yes
28	Yes
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	1150

Strong Points	*Areas of Improvement*
• Great job catering to intended audience, such as the note for non-technical readers in the vulnerabilities section and having the mitigation and explanations. Good use of color and organization for readability such as in the vulnerability section. • The vulnerabilities and mitigation table gave a lot of information which would make it easy for the "senior leadership" to follow. • Good explanations of vulnerabilities, suitable for executive presentation. Call out services/inventory impacted by remediation/hardening.	• The system overview was overly focused on the incident vs the system itself. • System overview spends too many words on the overview of the incident with little emphasis of the system and it's purpose, and wasn't geared to senior leadership. It needed to be more focused on the system overview itself. The colors in the asset inventory was good, but ended up making the table more clunky. The diagram gave an overview of the system but lacked in logical connections. • System overview was a bit unclear

Strong Points	*Areas of Improvement*
• The hardening section is excellent and shows clear understanding of real-world cybersecurity tools, processes, and reasoning. • I really appreciated the division of the different machines being very clear in each section.	• The report could briefly summarize the main takeaways or key metrics, such as how many vulnerabilities were fixed or which tools were most effective, to help readers quickly see the team's results. • Go more in depth with the hardening steps and not just what you did for the vulnerabilities stated in the previous section.

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	1002

Strong Points	*Areas of Improvement*
• Excellent opening - best seen. Very polished, obviously rehearsed and clean slides. • Great job all around, easy to follow along and you kept it at the C-suite level. Ending with the costliest option is to do nothing was a nice touch! • "The presentation started with a very strong presence and confidence from both speakers and that remained true through the whole slide deck. I am extremely impressed with the adept use of PowerPoint tools and the dedication to film this professionally and in a setting that lends us to believe this is truly corporate America. The presentation is marginally over 5 minutes but not so much that points could be reasonably lost. • The risks are summarized well and in an impactful manner. It would have been ideal to have a dollar value assigned to the ""financial impacts"" but noting that this rig provides the main source of crude oil for the entire Western region of the US supports the gravity and scope of the impact. • Able to identify risk and solution • Very professional and well displayed video. • well presented & good slides	• Provide more details on remediations (name/function of apps, cost, timeline). Use bullet points to supplement header graphics. Too few words - C-Suite expects to see numbers, graphs and more details. "Thank you" slide - instead say "we are available to answer your questions." • Points were deducted because not all strategies "relate to previously identified risks" because the hypothetical breach came from an approved vendor, doing approved work, in an area they were supposed to be in. And it is unknown if they are the attacker, or just the vector the attackers used to breach the oil rigs' systems. So access control and MFA buys no coverage for this specific scenario (but is always a good protection control in the real world). With that being said, intrusion prevention (and detection) tools would be beneficial, can be found open-source, and would prevent or contain future attacks and is therefore a better high priority recommendation that was touched upon in this presentation. • Please add in the financial impact to the company and detail explain how you come up with the solution • Would recommend that the second speaker, slow down a bit. Funding of recommendations was not addressed.

Strong Points	*Areas of Improvement*
	- telling the board about regulations regarding pollution they will be very aware of vs quantifying, and didn't cover costs of solution

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	250	250	0	125

Whack a Mole		
WAM1	WAM2	WAM3
125	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
1475	499

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	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
43667.81	97.04%

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
1352

Green Team Survey Comments
• The footer is visible on all pages except the homepage • Site loads slow. No manage users when logged in. • The footer on the home page needs to be lower, and the footer is not on every page (login page) • Footer is not at the very bottom of the page. • Admin button present • Good job • Good job • Fantastic Job Team 64! • Doing Great! • 5:43 This site can't be reached • 5:53 This site can't be reached