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

UNIVERSITY OF ILLINOIS CHICAGO

CYBERFLAMES

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 28 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	254	16.93%	83
Security Documentation	0	0.00%	93
C-Suite Panel	1087	86.96%	24
Red Team	0	0.00%	91
Blue Team	1180	59.00%	88
Green Team Surveys	0	0.00%	92
Deductions	0		
Overall	**2521**	**25.21%**	**92**

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	254

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

1		10.7	Yes	17	Yes
2	Yes	10.8		18	Yes
3		10.9		19	Yes
4		11.1		20	
5		11.2		21	
6		11.3		22	
7	No	11.4		23	
8		11.5		24	
9		11.6		25	No
10.1	Yes	11.7		26	
10.2	Yes	12		27.1	No
10.3	Yes	13		27.2	
10.4	Yes	14		28	
10.5	Yes	15	Yes	29	
10.6	Yes	16	Yes	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	0

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	1087

Strong Points	*Areas of Improvement*
• Speakers were well rehearsed and slides well-organized. Great job reasoning in the policy updates/strategy section and tying each update to the risk section. Also, great job ensuring the c-suite can understand all technical discussion, for instance describing what an access control list is.	• High priority actions had some cost associated. For instance, even if management are acting as instructors for staff training, staff time to listen/learn has to be paid for. • Some slides were packed with too much text to consume

Strong Points	*Areas of Improvement*
• Great analogy of a cell phone to access control list • I liked how you tied some of the strategy to event specifics. Weekly management reminders is a great way to keep cybersecurity on peoples mind, especially when they are likely already having pre job briefs. • Strategy to reduce risk was a strong point as the policy updates did address the outlined risks. Good to see both third-party vendor vetting and data protection policies at the top of the list. Strong justification given as a part of the expected outcomes slide. • The overall presentation was concise and clear. • The team presented strong visual aids and provided in-depth, well-thought-out recommendations. The use of analogies, such as comparing ACLs and whitelisting to a contact list, effectively helped translate technical concepts into business-friendly language. • Risks and mitigation strategy were very thorough	• Regarding the radio recommendation. We want to be cautious that we somewhat stay in our cyber lane, if you notice an operational issue you can phrase a recommendation differently and leave the specific implementation up to the appropriate group. For example, instead of recommending radios for $1000, your recommendation can be for the Operations group to establish a back up platform communications method to be used in the event of an outage. This way you flag an issue (backup comms) while acknowledging the Operations SMEs are the best ones to figure out what that looks like and cost. For example, oil platforms have many intrinsically safe areas so radios need to be Div 1 or 2 rated. A single intrinsically safe radio ranges from $700-$1100. Your $1,000 recommendation would likely end up being $20,000+ over budget. • Unfortunately, the presentation exceeded the allotted time by about five minutes. The slides could benefit from some refinement. Fore example, removing unnecessary images (such as those on the Policy Updates slide) would help de-clutter the content. Additionally, omitting key details from the slide text can make certain points confusing for a C-Suite audience. For example, under 'Danger to Employees', the only item listed was reputational damage. It would be more appropriate to address potential loss of life, litigation, and related safety concerns. It would also strengthen the presentation to explicitly highlight items with financial impact, such as regulatory issues tied to 'Environmental concerns'. • The students could be more confident and actively engage the audience. • While the explanations were clear overall, reducing the amount of technical jargon or simplifying terminology earlier in the presentation would make the content more accessible to a broader audience. • Try to avoid commercial technology such as walkie talkies for your high priority 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	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
1075	105

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)
0	0	27	26	27	0	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
9186.85	20.42%

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
0

Green Team Survey Comments
• Internal server error • Team 28's website is not functional. • "Illuminate\Database\QueryException • Database file at path [/var/www/html/database/database.sqlite] does not exist. Ensure this is an absolute path to the database. (Connection: sqlite, SQL: select * from 'sessions' where 'id' = iragfkYmgLYQNGqkonQ12lPuYBMr2fadgDfUmjGy limit 1)" • Site didn't load due to an internal server error. • Database file at path [/var/www/html/database/database.sqlite] does not exist. Ensure this is an absolute path to the database. (Connection: sqlite, SQL: select * from 'sessions' where 'id' = hSrTO4zv5VfVGsdBuFlayRCoqmDr8nbFtRGOuH06 limit 1) • This website does not open. The user is met with an 'Internal Server Error' message. • 'Internal Server Error', 'Database file at path [/var/www/html/database/database.sqlite] does not exist.' • "Accessing the page came back with the error below; 'Internal Server Error Database file at path [/var/www/html/database/database.sqlite] does not exist. Ensure this is an absolute path to the database. (Connection: sqlite, SQL: select * from 'sessions' where 'id' = iyhc9K75QQsoRmOSJOVZLF0znH3eHhMyPB4h4Yv9 limit 1)'" • site does not load • Internal Server Error when trying to access webpage • site won't load • 'Internal Server Error'. 'Database file at path [/var/www/html/database/database.sqlite] does not exist.' • unable to access site - Internal Server Error: Illuminate\Database\QueryException • Internal server error • Internal Server Error • Could not reach http://Web.blue0028.cfc.local Good luck! • Site is down • Internal Server Error • Your site doesn't load at 4:30 • Internal Server Error, site unavailable • 5:26 Internal Server Error • website is down • Site is down