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

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

SIGPWNY

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 80 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	727	48.47%	8
Security Documentation	1130	90.40%	25
C-Suite Panel	761	60.88%	89
Red Team	1500	60.00%	14
Blue Team	1990	99.50%	1
Green Team Surveys	1314	87.60%	12
Deductions	0		
Overall	**7422**	**74.22%**	**12**

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	727

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

1	No	10.7	Yes	17	Yes
2	Yes	10.8	Yes	18	Yes
3	No	10.9	Yes	19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6	No	11.3	Yes	22	
7	No	11.4	Yes	23	
8		11.5	Yes	24	Yes
9	No	11.6	Yes	25	Yes
10.1	Yes	11.7	Yes	26	
10.2	Yes	12		27.1	Yes
10.3	Yes	13	No	27.2	Yes
10.4	Yes	14		28	Yes
10.5	Yes	15	Yes	29	Yes
10.6	Yes	16	Yes	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	1130

Strong Points	*Areas of Improvement*
• System hardening section was easy to follow, well thought out, and comprehensive. • Very strong diagram. • Concise system description that considered senior leadership. • Threat Vulnerabilities • Network Diagram	• The system overview didn't discuss the system or its purpose, just the machines that made up the system. • Very strong. Possibly rely on a framework more towards the end in your methodology. • Try to ensure diagram legend is consistent for all server types.

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	761

Strong Points	*Areas of Improvement*
• The presentation was good and provided thorough details regarding the business and operational risks. • Great amount of explanation of the incident, risks, and recommendations and knowing the material of the presentation. • Good identification of risks, well done. • Strong point of this entry was definitely the identification of risks pertaining to the incident. There was a good delineation between operational and business risks. The presentation definitely reflects some level of technical aptitude. • Clear slide design • The approach to talking about risks is tied to the C-suites concerns. I like the pillars of visibility, remediation, and hardening. But strategy should be long term ways to reduce risk, not actions in the scope of 1-2 days.	• Areas for improvement include providing a strategy to reduce risks and outlining more long-term actions. Additionally, the high-priority recommendations need some additional detail, such as the reasoning behind the actions and the potential future risks if the recommendations are not followed. • More time of the content of the presentation. It was 4min 18seconds • Strategy was not explained for short and long term, recommendations were mixed up with strategy, difficult to follow the action plan. Team had more time not used to explained the missing parts. • The presentation appeared to lack an overall piece that would be strategic (not tactical) recommendations that the C-Suite could make in regard to long-term organizational or policy changes. The technical implementation seemed to be more of the high-priority recommendations, but the timelines were a bit short and pretty technical given the C-Suite level audience. Including information about financial impacts direct to the business bottom line would be a good improvement. It would also be beneficial to use more of the time to discuss risks of not implementing the provided recommendations. • risks should be quantified financially as well. • technical implementations being implemented in 1 day is an unreasonable timeline. Staff would need to be trained, software would need to be tested before deployment, deployment might only be possible during schedule downtime, etc. • You need to quantify risks R=L*I. You largely focus on impacts of your risks. Never say "won't cost us anything." Labor is a cost, even if you are using internal staff. Any hour addressing your proposed actions is an hour you are taking away from something else. How do your actions tie back to the risks you convey?

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	250	125	125	250	0	0

Whack a Mole		
WAM1	WAM2	WAM3
250	125	250

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	515

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
49076.67	109.06%

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
1314

Green Team Survey Comments
• your footer is just a little off! • footer text missing from home page. • there's no manage button when log in. • no manage button when log in. • Nice formatting. The only issue is that there is no footer on either the login page or the signup page. • All the elements are present. Good job! • green user deleted from user management • Amazing work! • Rock-solid work! Even Obsidian Rift’s rigs approved Unfortunately, you’re missing the footer on the login and signup pages. • Nice job Team 80! • I am unable to see the full image of the rig when the website opens up. In the User Management tab, you are missing the Green User but you do have the 2 admin users. Your rig has 'Normal Operations'. • website is down • This site can’t be reachedweb.blue0080.cfc.local refused to connect.