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

UNIVERSITY OF TOLEDO

UT CYBER SECURITY CLUB

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 94 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	474	31.60%	39
Security Documentation	1058	84.64%	50
C-Suite Panel	882	70.56%	77
Red Team	1375	55.00%	22
Blue Team	1887	94.35%	22
Green Team Surveys	1272	84.80%	33
Deductions	0		
Overall	**6948**	**69.48%**	**33**

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	474

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

1	Yes	10.7	Yes	17	Yes
2		10.8	Yes	18	Yes
3		10.9	Yes	19	Yes
4		11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	No
6	No	11.3	Yes	22	
7	No	11.4		23	
8	No	11.5	Yes	24	
9	No	11.6	Yes	25	No
10.1	Yes	11.7		26	
10.2	Yes	12	No	27.1	Yes
10.3	Yes	13	No	27.2	Yes
10.4	Yes	14		28	Yes
10.5	Yes	15	Yes	29	No
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	1058

Strong Points	*Areas of Improvement*
• Good job defining acronyms before shortening them and formatting tables/information cleanly for readability. • "The technical accuracy of most findings is good. • The report includes detailed coverage of Active Directory hardening, and the mitigations are appropriate and realistic. • The structure and writing are organized and easy to follow." • The vulnerability and hardening sections stand out for their depth, precision, and	• 'Senior leadership' audience should have been targeted more throughout the document. System hardening section warranted more justifications throughout. • "The report mentions an RDP vulnerability on port 3389, but the asset table lists this port as closed. This inconsistency should be clarified or corrected. • Severity levels should be added for each vulnerability. • Including a brief summary of key risks and verifying that all vulnerabilities match active ports would enhance overall accuracy."

Strong Points	Areas of Improvement
clarity, showing excellent teamwork and applied cybersecurity skill. • Great job on identifying many vulnerabilities and the descriptive mitigations. • Your grouping of known vulnerabilities was clear and well organized, and the formatting of your system hardening section was clean and effective. The structure of your work made it easy to follow and reflected a strong sense of presentation.	• The report could include a short executive summary to highlight major risks and fixes at a glance for non-technical readers. • System hardening does not have proper justification and is mostly a restatement of the known vulnerabilities section. • You delivered a well-rounded submission. Adding just a little more narrative explanation in a few places would make an already strong effort even more polished. You did an excellent job and it shows in your documentation.

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	882

Strong Points	Areas of Improvement
• The slides were thoughtfully designed, for instance the use of a table on the "High Priority Security Actions" slide was effective. • Good Visual aids. I like the High Priority slide. But don't be afraid to suggest something that costs money. You just need to justify it. • The high priority actions are well laid out with timelines, financial costs (if any), and how the actions mitigate risks mentioned previously. It's a clean, easily referenced table that conveys technical measures in a way anyone can understand. The risks of inaction are mentioned to further underpin the argument in the presentation. • Good work articulating the roles of the different team members. • Well designed slides. Good use of video embedded over slides. • Nice summary of risks due to inaction • Great job including the open-source tools that will be used for high impact action summary.	• It would improve the presentation to spend more time on slide 8 in particular (the communication and policy recommendations) and verbally elaborate more on the content of the slide. • While the discussion of business and operational risk was effective, it would benefit from a more explicit discussion of financial impacts in dollars. • It isn't sufficiently addressed how staff training or incident simulations could cost 0$. Wouldn't it cost some money for training materials/instructors and/or paying for employee's time during training? Also, high priority security actions could be better connected to the identified risks. • There is some use of technical language like 'ICS', 'IDS', 'VLAN', which should be 1) defined before being abbreviated and 2) explained in more depth so all members of the c-suite can follow along. • Video splicing was choppy. You could go a little deeper on the risks, and expand on the strategies. • The risks were summarized but there was not enough conversation regarding the impact to the company about operational concerns or quantitative financial impacts of those risks. The Communication & Policy

Strong Points	*Areas of Improvement*
	Recommendations could be considered a proposed strategy for reducing business risks but this isn't immediately clear. A strategy that is labeled as such and which clearly addresses identified risks and proposes methods to reduce them in the near and long term would enhance this presentation. • Risks should be quantified monetarily. • Timeframes are very tight. The security actions will need to be tested, and implemented possibly during downtime. Staff may need to be hired or trained. • Solutions aren't necessarily $0 cost as there will be staffing, testing costs, etc. • Risk of inaction is good to include as a final take away. • Did not include strategies to reduce risk. • Clearer understanding of long term actions • In preliminary findings, try to tie in the risks from previous slide to create a segue into strategy/high priority recommendations.

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	0	250	125	0	125

Whack a Mole		
WAM1	WAM2	WAM3
250	250	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	412

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
36069.23	80.15%

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
1272

Green Team Survey Comments
• extra admin acct
• Site looks good, but I had no access to the 'Admin Dashboard'. I could log in, but there was no 'Admin' button, it only returned me to the main screen.
• Check footer home page
• No user management when logged in.
• footer text missing from main page
• Some accent colors are wrong. Footer is missing from main page
• Red team has admin access.
• no footer on the homepage
• footer not available on main page. site colors are purple and yellow. red admin user added
• Footer is not on every page
• website is down