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

TENNESSEE TECHNOLOGICAL UNIVERSITY

CYBEREAGLES

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 27 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	645	43.00%	16
Security Documentation	1207	96.56%	10
C-Suite Panel	1152	92.16%	8
Red Team	2250	90.00%	1
Blue Team	1923	96.15%	14
Green Team Surveys	1232	82.13%	3
Deductions	0		
Overall	**8409**	**84.09%**	**3**

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	645

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

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

10.7	Yes
10.8	Yes
10.9	Yes
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	Yes
26	
27.1	Yes
27.2	Yes
28	Yes
29	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	1207

Strong Points	*Areas of Improvement*
• This is an impressive security documentation submission, the content is excellent and the overall readability is very professional. Every area is very thorough and professionally presented. The System Overview calling out IT and OT systems, Asset List, Network Diagram, Vulnerabilities and Mitigations are extensive and all excellent, but this is the best System Hardening report yet. The first section in System Hardening that addresses senior management and sets expectations them is perfect. The rest of the recommendations	• Overall, it's really difficult to think of any improvements, but if there were one thing, it could be to further develop the section of Future Detection and Monitoring with suggestions for a monthly patching and update plan, or another IDS/IPS monitoring system in addition to Wazzuh. • Asset inventory is complete but is hard to read as comma separated. Best to put Port/Service pairs on separate lines • system overview could have been a bit more organized

Strong Points	*Areas of Improvement*
and mitigations addressed are very well organized and includes Future Detection and Monitoring to maintain all the system hardening changes you have implemented, additionally the list of tools used at the end is very helpful. • Great job documenting the PLC and HMI vulnerabilities as future mitigations. Very thorough approach to system hardening plans. • Tables and vulnerabilities were well organized and easy to follow • Identified potential IT/OT boundary • The system hardening section was well laid out, easy to read, and thorough.	• Some sections were too technical for the audience. The first half of the hardening steps were actually just enumeration, not hardening. • Asset inventory could have been more thorough.

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	1152

Strong Points	*Areas of Improvement*
• Great job tying risk strategy back to a through list of operational and business risks • The team started out strong. • You did a good job of clearly explaining the risks you identified, as well as tying your risk prevention strategies and high priority recommendations back to those risks. • The strategies and recommendations were continually tied back to the business concerns and risks, which is important to the C-suit. • Overall, this presentation was well thought out and professionally done. • I really like how they structured their ppt, it was easy to follow and allowed for clarity	• It could help to provide more specific detail, such as $ estimates for risks and for high priority recommendations • The slide presentation needed some attention. • I would recommend including more detail in your slides. Your preparation was very well done, but visuals go a long way when presenting to a C-Suite! • I honestly do not have any feedback for these that need to be improved. • I would recommend including some sub-bullets of your main talking points for each slide to help the audience follow along both audibly and visually. • Consider color and font size for people's with sight issues. Their ppt content could have been a bit more detailed.

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	250	250	250	0	250	250

Whack a Mole		
WAM1	WAM2	WAM3
250	250	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
1420	503

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	25	27	24	23	23	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
43993.04	97.76%

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
1232

Green Team Survey Comments
• The logos in the navigation bar are alright but the obsidian rift one should be on the right instead of the left. • there's no 'User Management' button . • The logo is not in the required position. • Looking good! • No footer on login page. Excellent work otherwise! • Nicely done! • Good work! All intended areas are still accounted for within the website and no issues locating anything per the requirements. • looks good • Unable to connect to website (got a time out error) • Bad Gateway • "502 Bad Gateway nginx/1.19.0" • Site is down