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

EAST TENNESSEE STATE UNIVERSITY

CYBERBUCS

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 26 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	361	24.07%	62
Security Documentation	1039	83.12%	53
C-Suite Panel	1093	87.44%	21
Red Team	750	30.00%	53
Blue Team	1883	94.15%	27
Green Team Surveys	785	52.33%	59
Deductions	0		
Overall	**5911**	**59.11%**	**59**

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	361

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

1	No	10.7	Yes	17	Yes
2		10.8	Yes	18	Yes
3		10.9		19	Yes
4	No	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6		11.3	Yes	22	
7		11.4	Yes	23	
8	No	11.5	Yes	24	No
9		11.6	No	25	
10.1	Yes	11.7	Yes	26	
10.2	Yes	12	No	27.1	No
10.3	Yes	13		27.2	
10.4	Yes	14		28	No
10.5	Yes	15	Yes	29	
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	1039

Strong Points	*Areas of Improvement*
• Well written system overview and good justifications for system hardening steps. Good use of GIT • comprehensive list of vulnerabilities and mitigation • Excellent detail and clear evidence of real remediation work. • Tables were easy to read and had consistent formatting • I think the System Hardening recommendations	• Need to clarify whether the PLC/HMI mitigations are just proposed for future fixes as these assumed breach systems may not be modified. Should be more specific in System Hardening section that the SIEM is Wazuh and talk about how it is set up externally. • system overview could be better communicated for a senior leadership audience who are less familiar with technical jargon

Strong Points	Areas of Improvement
	• Tailor the language for an executive audience. Include key takeaways rather than step-by-step actions. • Consider senior leadership more carefully for content and formatting.

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	1093

Strong Points	Areas of Improvement
• Great job tying risk strategy back to a through list of operational and business risks • I really enjoyed your visual aids. • Liked your chart of risks and how you assigned owners to your mitigation strategy and recommendations. • 100% Risks. Excellent use of an impact-probability matrix to assist with explanation to C-Suite. Great to see that financial concerns were kept in mind as a part of the risk threat assessment. Good approach align the strategies to reduce risks by the numbers that have been established with the corresponding risks. • You did a thorough job of explaining the situation and laying out your solution. • Amazing engagement of risks within your mitigation strategy.	• No mention of costs to implement • the second presenter was just reading from the slides • A bit too much time was spent on the introduction and overview. The slide on the Presentation Outline could easily be removed to give more “breathing room” for the key sections on risk reduction strategies and high-priority recommendations. Those sections felt somewhat rushed, and a more balanced allocation of presentation time would have helped. As a result, some of the recommendations and strategies came across as incomplete or lacking consistent supporting reasoning. • The presentation felt rushed and information was crowded onto the slide. To make your points more clear and to slow down pacing, consider putting each point on it's own slide and talking to the point instead of putting everything you are going to say on the slide. • Remember to explain how each high priority actions reduces future risk.

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	0	0	0	0

Whack a Mole		
WAM1	WAM2	WAM3
250	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
1405	478

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	22	23	25	24	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
41813.11	92.92%

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
785

Green Team Survey Comments
• no admins • The users 'blue@obsidianrift.oil' and 'green-admin@obsidianrift.oil' do not have the admin tags. • Site looks good, but I had access to the 'Admin Dashboard', the 'Admin' button was still showing. Under 'User Management', there were 'No users found'. • No Admin users are listed in the 'Admin: User Management' page. Only green-user@obsidianrift.oil user was listed as User but no Admins. • users missing • nginx error mid survey • "Things were going so good. It looks you got hacked in the middle of my evaluation :-(• Oh hold on, your back. Way to fight off the attacker! I have Admin access as a normal users. I don't see any Admin users in User Management when logged in as Admin. Design is good. Even a footer on the Home Page." • The website does not load. The user is met with an 'Internal Server Error' message. • 'Internal Server Error'. 'Connection refused' • this site is down as well • this site is down • Site does not load • Site is down • Unable to connect: Internal Server Error - Illuminate\Database\QueryException - IP not allowed to connect to this MariaDB server • 5:46 This site cant be reached • Site is down