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

THE UNIVERSITY OF DALLAS

GROUNDHOGS

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 47 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	533	35.53%	25
Security Documentation	1112	88.96%	34
C-Suite Panel	1105	88.40%	16
Red Team	375	15.00%	77
Blue Team	1609	80.45%	58
Green Team Surveys	1208	80.53%	58
Deductions	0		
Overall	**5942**	**59.42%**	**58**

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	533

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	No	10.9		19	Yes
4		11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	Yes
6		11.3	Yes	22	
7		11.4	Yes	23	
8		11.5	Yes	24	
9		11.6		25	
10.1	Yes	11.7		26	
10.2	Yes	12		27.1	Yes
10.3	Yes	13		27.2	Yes
10.4		14		28	Yes
10.5	Yes	15	Yes	29	
10.6	No	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	1112

Strong Points	*Areas of Improvement*
• Network diagram is clear and informative • Good network diagram and inventory. • It has a strong system overview and asset inventory. • The system hardening section demonstrates excellent structure, depth, and clarity, showcasing a mature understanding of proactive defense and secure configuration. • The system hardening section was well developed and thorough.	• Differentiate between mitigations and hardening activities. Include identified vulnerabilities in the assumed breach machines - can state that no mitigation was allowed or list future actions. Start overview by stating the purpose of the system overall. • More vulnerabilities needed to be listed. • Extend the vulnerability and hardening coverage specifically to HMI and PLC. • The asset inventory and vulnerability sections could more explicitly highlight risk prioritization or business impact, helping leadership understand which systems

Strong Points	Areas of Improvement
	posed the greatest threats before mitigation. • In the system overview section, it would have been better to give a very general overview of the company and what the systems do.

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	1105

Strong Points	Areas of Improvement
• Risks to Core Business • Really well done all around, was at the right level for the C-suite. • The information is presented professionally. • Your high priority recommendations were practical and cheap. • Ryan did an excellent job of mentioning team members not present. Very clear slide deck and analyzed 3 core business risks and strategies. Overall synopsis was great of incident cost, procedural gaps, key equipment with faulty automation commands resulting in risk. Response budget was clear and defined. Reset passwords, etc. provided data for costs of savings and semi-annual security training for employees to prevent human error.	• The High Priority Recommendations could have been more detailed • Regarding Risk 2, I was surprised to hear such pointed language used as if this was a deliberate malicious act by your vendor. As an assessment team we want to frame the situation with facts and neutral tone. The distinction between intentional acts and negligence is important, it affects legal liability, relations, and the credibility of your team and the organization. • There was little emphasis on the financial bottom line. • These risks are heavily mixed with cybersecurity jargon. The C-Suite cares about operational risk, not about what vulnerabilities in the system led to the incident.

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	0	0	0	0	0	0

Whack a Mole		
WAM1	WAM2	WAM3
125	125	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
1350	259

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)
21	21	26	26	27	22	27	27	27	20	26

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
22648.97	50.33%

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
1208

Green Team Survey Comments
• Home Page is too zoomed in (please zoom out). Great work!
• Site looks good, but I had no access to the 'Admin Dashboard'. I could log in and there was no 'Admin' button, but it only returned me to the main screen.

Green Team Survey Comments
• no footer on home page. • No footer on the home page. • "I was able to get Admin to showup in a drop down menu by resizing browser with a normal user; however trying to access that page gave me Error 403 - Good job! It looks like a red user was added to the user list - oops :-(… and I could promote them to Admin … double oops :-0 … but I could delete them … redeemed!!! • footer not on main page • There is no footer on a home page • Suggest adding footer to home page • Address footer is supposed to be on every web page, but it's not found on the home. • No footer on homepage, Login, or Sign Up. Nice work otherwise! • Missing footer on homepage, other than that it looks good! • Good job • 5:29 Internal Server Error • Internal Server Error, site is unavailable • site cannot be reached