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

UNIVERSITY OF PITTSBURGH

CYBERPANTHERS

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 32 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	294	19.60%	76
Security Documentation	750	60.00%	86
C-Suite Panel	919	73.52%	69
Red Team	375	15.00%	77
Blue Team	1501	75.05%	65
Green Team Surveys	183	12.20%	85
Deductions	0		
Overall	**4022**	**40.22%**	**85**

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	294

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

1	No	10.7	Yes	17	Yes
2		10.8		18	Yes
3		10.9		19	Yes
4		11.1		20	Yes
5	Yes	11.2		21	
6		11.3		22	
7	No	11.4		23	
8		11.5		24	No
9	No	11.6		25	
10.1	Yes	11.7		26	
10.2	Yes	12		27.1	No
10.3	Yes	13		27.2	
10.4	Yes	14		28	
10.5	Yes	15	Yes	29	
10.6	No	16	Yes	30	

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	750

Strong Points	*Areas of Improvement*
• Asset inventory is sound. Hardening steps were well explained. Easy to read document except for beginning italics. • The asset inventory was organized well. • System Hardening section was written well since it was thorough and had justifications.	• System overview should not be in italics; should focus only on its design, not it's hacked state. System diagram missing legend; missing router; assumed breach VMs are part of the same subnet as the other 4 VMs; subnet IP address is wrong (no x); all 6 VMs are outside of subnet range. Vulnerability listing is <23 of build vulns. Hardening had 3 of the 4 steps needed for a perfect score. • The system overview could have used more detail.

Strong Points	Areas of Improvement
	• Keep your hostnames and formatting consistent (e.g. Task Box, italics). Check what machines you can and can't harden. Read over your system overview to make sure everything sounds like it makes sense. Make sure your network diagram is absolutely clean.

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	919

Strong Points	Areas of Improvement
• The contents of the strategy slide were well thought out. • The students provided a solid quantification of risk and demonstrated good use of technical language identifying specific tools they will need upfront to implement their proposed solutions effectively. • Good suggestions for priority recommendations and having everyone help present together. • I liked that all team members presented. • I loved the design of the presentation. You did a good job of laying out and communicating your recommendations visually, which is a strong skill when communicating with executives that may be non-technical. Good work! • High priority actions were better.	• Approximately two minutes was spent on the situation report – this was too long. The situation report overlapped with the risk section, for instance describing environmental harm and loss of data. It's best to separate the situation description from the risk section more clearly and shorten the situation report. • Slides were too wordy in general. It's best to keep the words on the slide brief and speak more to the points. • The high priority items needed to be shortened into 3-4 items that you feel are the most important. Additionally, item 3 should not have background checks on suppliers as well as training and awareness in the same point. Overall, the contents of the strategy slide seemed to be a better representation of high priority (immediate) action items where the 'high priority' slide seems better as the long term strategy rubric item with policy updates like the background checks and item inventory. • The presentation would be stronger with less reading and more storytelling to engage the audience. Incorporating more metrics and data-driven examples would also enhance credibility and clarity. • Strategy is tied too much to the incident and is not tied back to operational and business risks. Too much text and too small on slides, impossible to consume. Unclear what individual contributions or roles were.

Strong Points	*Areas of Improvement*
	• Presenters should introduce themselves when first talking. Also, second presenter appeared to be spinning in the chair, which was distracting. Some slides had too much information. • There were a few distracting moments, particularly the wind noise in the opening segment, as well as a few video cuts that seemed sudden. • You need to explain how your mitigation strategy directly addresses identified risks.

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 point*s. 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 point*s. 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
0	0	0	0	0	0	125

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
1475	26

Each team was scanned *27 time*s 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
2306.34	5.13%

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
183

Green Team Survey Comments
• This site is compromised: color theme is wrong, careers page shows wrong text, footer is wrong, tagline is wrong, no Admin.
• Background color is gold/goldenrod. Nav bar is missing logos, login button, and the company name is incorrect. Wrong background image. Tagline reads 'Spilling oil is Good. Spilling Data is better.' No positions listed in Careers. Footer text is missing a street address and city. Rig status page goes to Internal Server Error - Illuminate\Database\QueryException
• Unable to login
• Most functions are dead.
• site not loading
• Wrong color assets, no oil rig image, missing footer, cannot log in, missing logos, missing career listings, rig-status page unavailable
• Accent color is gold/goldenrod. Nav bar is missing logos, login button, and the company name is incorrect. Wrong background image. Tagline reads 'Spilling Oil is Good. Spilling Data is better.' No positions listed in Careers. Footer text is missing a street address and city. Rig status page goes to Internal Server Error - Illuminate\Database\QueryException - Connection Refused
• site is wrong color, careers not listed, no login button, rig status page does not load, no logos or picture
• no homepage footer
• no homepage footer
• Wrong color, footer has incorrect info, company name is wrong, careers missing, rig status is unavailable, and admin users are missing. Also logos are missing.

Green Team Survey Comments
• "This site cant be reachedweb.blue0032.cfc.local refused to connect. Try: Checking the connection Checking the proxy and the firewall ERR_CONNECTION_REFUSED" • 5:51 This site cant be reached