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

THE UNIVERSITY OF TEXAS AT SAN ANTONIO

THE ROADRUNNERS

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 86 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	922	61.47%	1
Security Documentation	1203	96.24%	11
C-Suite Panel	1165	93.20%	6
Red Team	2125	85.00%	2
Blue Team	1885	94.25%	26
Green Team Surveys	1426	95.07%	2
Deductions	0		
Overall	**8726**	**87.26%**	**2**

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	922

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

1	Yes
2	Yes
3	
4	Yes
5	Yes
6	Yes
7	No
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	Yes
11.7	Yes
12	
13	
14	Yes
15	Yes
16	Yes

17	Yes
18	Yes
19	Yes
20	Yes
21	Yes
22	
23	
24	
25	
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	1203

Strong Points	*Areas of Improvement*
• Good job writing acronyms out before using the shortened versions. Also, breaking longer sections such as the system hardening section into shorter subsections was effective for readability. Great network diagram. • Very good document from Team 86 • Excellent network diagram, excellent calling out justification clearly. • The report was very professional and comprehensive. • Super detailed vulnerability mitigation steps and great network diagram	• Ensure to keep formatting consistent throughout on small details, for instance using italics for some but not all parts of the asset inventory table. Also, some parts could have been better tailored to the 'senior leadership' audience. • It can be improved tailoring more for executives. • Vulns could have had mitigations in more appropriate language for senior leadership. • At 28 pages, this report might be considered too long and too detailed for a c-suite audience.

Strong Points	*Areas of Improvement*
	• System hardening steps and format could be simplified rather than separated into phases

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	1165

Strong Points	*Areas of Improvement*
• Excellent articulation of operational, financial, and safety risks tied to business outcomes; professional and clear executive framing. • I like the interactive presentation. • Good work identifying the work completed by the different team members. • Nice use of green screen to show the speaker on the slide. • Nice use of embedded closed captions. Would recommend using a higher contract color as the slide background color is the same color as the font. • Good work including an estimated timeline. • Good work encouraging viewers to reach out with questions. • The presentation met all the requirements with flying colors. An exceptional team that proves that they have prepared thoroughly; which is why I want them to win. • Bravo, Xander, Kevin, Marco, Jacob, Ian, Fardeen! • Excellent description of risks and business impact. Good job including all costs - labor is often overlooked. • Well done on high priority actions. They were easy to read and clear on their goal.	• Could briefly condense technical depth — might overwhelm a C-suite audience with detail. Video quality was exceptional. • Please be detail of the financial impact before and after using C-Suite • Risk should be quantified financially. • Reducing Risk: should go slower and provide more details, and justifications. • Also should discuss who will do theses tasks and associated costs: staffing, software, hardware. • High priority actions: also speak a little slower. Cost estimates seem low. New staffing or consultants may need to be hired. • Could include a references slide to encourage further research. • I can't suggest any improvements, at least not for this presentation. • Strategy slides felt a little busy and editing was a little distracting at times. The presentation felt a little rigid - like reading from a script. • The slides have too much going on in such a short period of time.

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	125	250	125	125	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
1450	435

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	25	24	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
38012.52	84.47%

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
1426

Green Team Survey Comments
• Meets all of the requirements. But Home Page footer is fixed in the middle than at the bottom. • Good job keep it up • Every component is present and working as expected on this web site. • Excellent work! • Great job! You secured that oil rig so tight even the crude couldn’t slip past you! • "502 Bad Gateway nginx/1.28.0"