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

UNIVERSITY OF HOUSTON

SHASTA SHIELD

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 79 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	344	22.93%	66
Security Documentation	1054	84.32%	51
C-Suite Panel	910	72.80%	74
Red Team	375	15.00%	77
Blue Team	1360	68.00%	82
Green Team Surveys	1172	78.13%	75
Deductions	0		
Overall	5215	52.15%	75

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	344

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

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

10.7	
10.8	
10.9	
11.1	
11.2	
11.3	
11.4	
11.5	
11.6	
11.7	
12	
13	No
14	
15	Yes
16	Yes

17	Yes
18	Yes
19	Yes
20	Yes
21	
22	
23	
24	Yes
25	
26	
27.1	
27.2	
28	No
29	
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	1054

Strong Points	*Areas of Improvement*
• Excellent system overview. Best job on vulnerability identification of 8 teams. • The known vulnerability section had just the right amount of detail. • The report was technically sound and well put together. • Everything is a strong point here. Congratulations!	• Asset listing should have just VM names in 1st column; no IPs. Network diagram has incorrect subnet (should be /26). IP address for switch not listed. "Pardue" is misspelled. • The system overview used too much technical language. The term is "Purdue Model," not "Pardue." The word "Confidential" is actually used in government documentation and should probably not be used here to make sure there is no confusion. • The hardening section could have been more tailored to a c-suite audience, the

Strong Points	*Areas of Improvement*
	mitigations didn't say what was actually done. - A little more attention.

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	910

Strong Points	*Areas of Improvement*
- The professionalism and they treated it like a real-world presentation to a board or C-Suite - I like that you had all members on the presentation. - You did a good job tying the risks you identified to your risk reduction strategies and high priority recommendations. - The long-term recommendations are tied back to the risks, but not really any justification in how. - The team delivered a solid presentation, demonstrating good technical knowledge and communication skills. It was great to see everyone present and engaged in the recording. The strategy to reduce risks was well thought out and thoroughly explained. - Exhaustive risk identification	- More technical details of the security tools or systems they will put in place and what is the roadmap for recovery look like? If you plan to implement an improved Endpoint Detection & Response like CrowdStrike it would save the company 4.3 million dollars in protecting assets and users. - More details on the risks and strategies. - I'd recommend more visuals to illustrate points like operational/financial impacts. These strongly help convey information to C-Level executives and can also help you develop more specific talking points. - You listed business impacts. That is only half of the equation of risk. What are the cost estimates for your high priority and long-term recommendations? - Keep up the good work. Continue refining your delivery and look for ways to make your visuals or examples even more engaging to further strengthen your presentation. - risk mitigation strategy and high priority recommendations needed more justification and connection to 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 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
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
1360	0

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	24	23	24	24	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
0.00	0.00%

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
1172

Green Team Survey Comments
• Unable to login

Green Team Survey Comments
• Unable to login, immediately crashes webpage • Site looks good, but I had no access to the 'Admin Dashboard'. When trying to log in, there was only an option to refresh the webpage due to the page being expired. • check your logos and colors! otherwise, the entire site seems a little off, and the image in the background is incorrect. • Header logos are in wrong locations • Looks like a website in recovery. Formatting meets minimum standards. But, everything works. • footer accent color is blue • unable to go back to the main screen after leaving it • The navigation bar does not send you back to the home page. The website is also very slow to run. • Exceptionally done Team 79! I especially like the Oil Rig Status webpage! • your navigation bar, logos, and background image are incorrect. • Great job cool unique website. • take out the home page on the top bar • 5:44 This site can’t be reached • website is down