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

SAM HOUSTON STATE UNIVERSITY

BA$H

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 8 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	219	14.60%	87
Security Documentation	996	79.68%	61
C-Suite Panel	1071	85.68%	29
Red Team	750	30.00%	53
Blue Team	1320	66.00%	85
Green Team Surveys	943	62.87%	73
Deductions	0		
Overall	5299	52.99%	73

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	219

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

1	No	10.7		17	Yes
2		10.8		18	Yes
3		10.9		19	Yes
4		11.1		20	Yes
5		11.2		21	
6		11.3		22	
7	No	11.4		23	
8		11.5		24	No
9	No	11.6		25	
10.1		11.7		26	
10.2		12	No	27.1	No
10.3		13		27.2	No
10.4		14		28	No
10.5		15	Yes	29	
10.6		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	996

Strong Points	*Areas of Improvement*
• Good, clean write-up. • Very readable and practical. It felt like a real-world report. • Excellent comprehensive documentation with clear system overview targeting senior leadership. Strong asset inventory with complete details for all hosts. The system hardening section demonstrated thorough understanding with detailed justifications using appropriate open-source tools. Professional formatting and technical terminology throughout.	• The network diagram only showed tunnels, not the rest of the connections. It also appeared that team did not have the time identify and list more vulnerabilities. • Could've briefly summarized the impact of fixes on overall security posture. • Consider including a visual network diagram with legend for full exemplary marks in that category. Could expand the vulnerabilities section to provide more quantitative metrics (number of CVEs addressed, severity ratings). The documentation would benefit

Strong Points	Areas of Improvement
	from including specific version numbers for the tools used.

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	1071

Strong Points	Areas of Improvement
• The justifications for each long-term strategy recommendation on the slide were effective. Speakers were well rehearsed. • The quality of the visuals is good, they are clean, simple and easy to follow as the speaker presents. The team did provide an exemplary overview of the operational and business risks in a clear manner that explained the precise impacts to the organization. While there is some jargon used in the slide, the presenter did not use it in his presentation showing clear mastery of the material and presented even the jargon in a manner that any C-suite exec. could understand. • Nice summary of operation and business risks including costs • Very clean and to the point. • Strong presentation, problem statement was explained well. The actions recommend made sense, they I term plan is well explained, using open source tools and plans that require adequate funding. • The presentation was clear, clean and professional.	• Cost of long term strategies could have been addressed in more depth—for instance, you mentioned training staff as part of the 'zero trust' section of the long term strategy recommendations slide but cost of such measures is important to c-suite members. • This presentation is almost six minutes long and while there are two clear presenters, acknowledgment of other team members is not given. There is no recorded video of the speakers so judging dress code cannot be completed. The team proposed four long term solutions but only listed three on their slides. They are recommending a SIEM system which would require additional funding. One note I would make is that demanding third-party vendors cannot use their own tools to perform their work is infeasible. • Including discussion of future risks if recommendations not followed • Possibly too technical, but very good in call other respects. • Consider the ppt color deck, it's too dark, the team members are not visible, was not able to tell who was talking or grade attire. • The team could have utilized visuals to enhance the message.

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	125	0	0	0	0	0

Whack a Mole		
WAM1	WAM2	WAM3
125	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
1320	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)
0	27	27	22	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
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
943

Green Team Survey Comments
• Operational :), no footer on homepage • Site looks good, but no logos and no 'Admin Dashboard'. • missing users with admin status. no logos • The admin users are not displaying in user management, the footer is incorrect, rig-status page as a custom handwritten image, and logos are missing in header. • Homepage needs a footer. No logos in header. Blue & green admins are missing from admin page • no logos, operation page is drawn, footer is missing on the home page, blue@obsidianrift.oil and green-admin@obsidianrift.oil do not have admin tag and no logos • no logos, no footer on the homepage, blue@obsidianrift and green-admin are not tagged as admin • No green or blue admin users, incorrect footers and not appearing on the home page, rig status dashboard not showing correct results, no logos in the header • Admin accounts not listed in users, address footers missing from home page, oil rig status page not as expected, logos missing in header. • I was able to log in with green-admin@obsidianrift.oil, but under user management there are no admins listed. No footer on home page, Login, or Sign Up. Rig Status page reads 'Operational :)' in handwritten script, this doesn't meet the 'Normal Operation' or 'Not Operational' requirement, but it was almost an effective workaround to meet the written requirements. No logos in header. • company name misspelled, admin users not showing up on user management, URL in footer • Site is down