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

UNIVERSITY OF SOUTH ALABAMA

DAYZERO

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 38 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	362	24.13%	61
Security Documentation	1100	88.00%	39
C-Suite Panel	984	78.72%	49
Red Team	875	35.00%	44
Blue Team	1912	95.60%	17
Green Team Surveys	1216	81.07%	47
Deductions	0		
Overall	**6449**	**64.49%**	**47**

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	362

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

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

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

17	Yes
18	Yes
19	Yes
20	Yes
21	
22	
23	
24	
25	No
26	
27.1	No
27.2	
28	Yes
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	1100

Strong Points	*Areas of Improvement*
• The team invested great effort in exposing and listing all the vulnerabilities and mitigation suggestions. The system hardening was thorough and well presented. All of the assets, ports and protocols, network diagram were presented well. • great job organizing and structuring your answers • The document was thorough. • detailed vulnerability identification and mitigation work that demonstrates deep understanding of system defense.	• It is evident that the team spent some time and effort to investigate the scenario and provided thorough explanations for mitigations and system hardening, but the overall presentation could be made more professional with just a bit more attention to detail; a few items include: the blank white pages left in the report, the help text from the report template is left in the report in a couple places, and the formatting of information presented could be improved. For example, in the System Hardening section, instead of providing a list of all the

Strong Points	*Areas of Improvement*
• Extensive vulnerability enumeration	tools used, consider providing the tools used for each section of the System Hardening description. One final thing noted in the System Overview, there are quick descriptions provided for each of the 6 components listed on the network, but the Task Management server description is missing even though it is mentioned above with the other components. • there were blank pages and some grammatical errors • Network diagram is missing connection to the internet. Some steps of the hardening section were too verbose, while justification was not included for others. • The system overview and hardening sections could better emphasize risk prioritization and summarize findings for a senior-leadership audience to strengthen executive communication. • Senior leadership might not understand some technical terms. Consider how technical content might be made more accessible to an audience without your expertise. Consider that they're likely interested in knowing how your system and recommendations fit into the broader business.

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	984

Strong Points	*Areas of Improvement*
• Crucial Recommendations • good summary of what happened. • Also, I like the bar chart of costs, but you may be a bit optimistic in your values. • Able to identify risk and taggle through the solution in detail • Including estimated timelines along with strategy and recommendations was a nice touch. The direct communication style used in the presentation is typically appreciated by leadership teams. • Great overall information re: how the incident occurred. Great data provided (i.e.	• They should include a roadmap and also missing some technical details / examples • More thought is needed for the risks and the strategy to fix those risks. • No ties between the risks and then the strategies to reduce or high priority recommendations. • Show more detail in graphs • The presentation felt a little rigid - like reading from a script (no points deducted). Slides could use a little polish (no points deducted). Consider prioritizing health and safety more strongly when identifying risks.

Strong Points	*Areas of Improvement*
timelines, window of operational disruption, etc. Operations in unsafe conditions, on-site awareness and restrictions of "spreadsheet base" for role based badge access was great add.	Recommendations should have stronger cost justifications and relate more directly to the scenario.

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	125	125	250	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
1475	437

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	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
38265.00	85.03%

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
1216

Green Team Survey Comments

- 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.
- Title says 'Obsidian Energi Co.', should say 'ObsidianRift Energy Co.'. Also wrong in the footer. Red team has admin tag.
- Red team has admin access
- You may want to put the footer on the home page and watch out there is a red user with admin access
- missing footer text from homepage
- footer missing from homepage
- no footer on the home page
- Energi
- No Footer on Home Page.
- Hello Team 38 the footer was missing on the main page. Other than that good job!
- Red team has admin, footer missing on homepage, and title should be 'ObsidianRift Energy Co.'
- The company name is spelled wrong in the header, the footer is not on every page, more admins than there should be in the admin panel.
- Red team has admin tag and missing footer on home page
- This site cant be reachedweb.blue0038.cfc.local refused to connect.
- Site is down