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

DAKOTA STATE UNIVERSITY

DSU TROJANHORSES

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 41 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	424	28.27%	50
Security Documentation	1125	90.00%	27
C-Suite Panel	918	73.44%	72
Red Team	500	20.00%	70
Blue Team	1475	73.75%	68
Green Team Surveys	1375	91.67%	60
Deductions	0		
Overall	**5817**	**58.17%**	**60**

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	424

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

1	No
2	
3	
4	
5	
6	
7	
8	
9	
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	
11.1	Yes
11.2	Yes
11.3	Yes
11.4	Yes
11.5	Yes
11.6	Yes
11.7	Yes
12	
13	
14	
15	Yes
16	Yes
17	Yes
18	Yes
19	Yes
20	Yes
21	Yes
22	
23	
24	
25	
26	
27.1	No
27.2	Yes
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	1125

Strong Points	*Areas of Improvement*
• Solid documentation is presented in an accessible manner. • This report was very professional and well written beginning with the System Overview which provides a great top level description of the scenario and the areas of concern. The asset inventory and network diagram were very thorough and well presented. The list of vulnerabilities and mitigations was detailed and appropriate for all the components. • The vulnerabilities and mitigations are comprehensive, well organized, and show	• Perhaps group and consolidate some details to increase understanding of vulnerabilities and connection to hardening activities. List of tools is missing from system hardening • The only area that could more professionally presented is System Hardening. While each component is mentioned and the improvements suggested, it is presented in long form list but could be made more readable in a table format, organizing the critical information for each component, mitigation, policy or procedure, and the

Strong Points	*Areas of Improvement*
excellent awareness of system-wide security practices. • The team produced a solid deliverable with strong organization and a clear understanding of the system. Your hardening work stood out, and your presentation showed that you approached the task thoughtfully and with good awareness of the project requirements. • Overall very strong entry, great network diagram	tools used to accomplish the system hardening task for each suggestion or component. • The system hardening section could include more justification for each major control or tool choice to highlight strategic reasoning behind the team's defensive approach. • Your work shows a solid understanding of the environment, and you're clearly on the right track. You already have a strong foundation just a little more specificity will help bring the full picture together. Keep building on this momentum; you're very close to an excellent, well-rounded submission. • The system hardening section could have used more technical details

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	918

Strong Points	*Areas of Improvement*
• Balanced treatment of financial, operational, and reputational risks. Presentation gives solid articulation of response tiers (monitoring, isolation, MFA). MFA might be hard to implement on existing OT systems. Polished and exceptional presentation and video inserts. • Good mentioning need to buy energy to replace that not produced. Included all presenters well and transitioned between presenters well. • Very professional presentation. Realistic timelines for recommendation implementation. • Identify risk and develop a detail solution • The presentation is suitable for all members of the C-suite • Involving your entire team in the video process was a great touch that led to a high-quality video. You did a great job of identifying business/operational risks, and tailoring your recommendations to those risks!	• The presentation could be improved by briefly summarizing each recommendation at the end for extra clarity and impact, ensuring the C-suite leaves with a concise list of next steps. • No ties between strategies / recommendations and identified risks. Slides were all different template, slightly jarring. Minor issue - mention your team number verbally! • You probably don't need to explain energy market buyback to the C-suite, but addressing it at all is a positive. Not all risks clearly tied back to the bottom line in concrete ways. • Discussion about how that risk impact on the company financial • High priority recommendations following strategy have areas where they don't necessarily overlap. Recommendations also appear like they will require additional funding and time for implementation.

Strong Points	*Areas of Improvement*
	• This is very nit-picky, but you could have focused a bit more on financial impact when identifying your 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	125	0	0	0	125

Whack a Mole		
WAM1	WAM2	WAM3
125	0	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	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)
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
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
1375

Green Team Survey Comments
• Footer Text not located on homepage. Logos for ObsidianRift/Abyssal Pearl do not match the Green Team Documentation. • footer is not on home page. • There is no footer on a Home page • logos- images match but the color is inverted. the footer page is available on the other pages except the home page • Logos are in the wrong location and wrong color • The footer is not on every page. The logos do not appear on the admin page. Additionally, the logos are not actually in the navigation bar; they are before it. • Recommendation to put the footer on home page and check your logo placement the documentation has the logos around the company name in the header. • Logos sometime disappear. (Located at Admin:User Management) • 4th user (yellow) listed when checking for Admins that was not on example. • logo is present but the image is inverted. the footer is not present on the homepage • Footer missing from homepage, and logos in the wrong location on the navigation bar. • Hello Team 41, the footer text was missing on the main page. • Footer not on every page - when login check your logos they get lost • missing footer on home page and logos are in the wrong location • footer is partially out of view on home page