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

KANSAS STATE UNIVERSITY

K-STATE CDC WHITE

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 77 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	355	23.67%	63
Security Documentation	1109	88.72%	36
C-Suite Panel	1017	81.36%	45
Red Team	1375	55.00%	22
Blue Team	1427	71.35%	78
Green Team Surveys	666	44.40%	57
Deductions	0		
Overall	5949	59.49%	57

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	355

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	Yes	11.1	Yes	20	
5	No	11.2	Yes	21	
6	No	11.3	Yes	22	
7		11.4	Yes	23	
8	No	11.5	Yes	24	Yes
9	No	11.6		25	
10.1		11.7		26	
10.2		12		27.1	
10.3		13		27.2	
10.4		14		28	
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	1109

Strong Points	*Areas of Improvement*
• The hardening section stands out for its depth and strong use of real-world security tools and techniques. • System hardening was well thought out and comprehensive. • Identified and justified future actions for when team is on-site for mitigations on critical HMI/PLC systems	• Some mitigation steps are listed as pending; fully completing and confirming these actions would strengthen the report's overall impact. • There was a duplicate IP in the network diagram. • Most of the "hardening" steps aren't actually hardening, just enumeration and remediation. No details were provided on the hardening steps mentioned.

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	1017

Strong Points	*Areas of Improvement*
• The slides were concise and clear. It is clear that speakers were well-rehearsed. The risks section in particular was effective and were clearly tied risks to financial concerns. • nice use of visuals! • The presentation is well thought out and explained by the presenters. They propose a reasonable strategy that applies to the identified risks that range from immediate actions to long term actions, all of which will improve the overall security posture of the company. The high priority actions range from short term steps to introduce immediate improvements and longer term actions that will provided continued support. The actions do require significant additional funding but this is framed within a comparison of what another future attack could cost the company if the investment is not made now. It is a subtle reference to a return on investment framed in money that would not be lost rather than revenue gained. It's an interesting approach. • clean slides • Good job at quantifying the impact of risks. I love the way your strategic plan is presented. Good job comparing the immediate action costs to potential loss. • I enjoyed the overall description of the use case. Slide deck was clear and easy to follow. Great use of references also provided at the end of the presentation. RRR: Recovering, Reinforcing and Resilience was a great reference to "See Something, Say Something" awareness. Cost and Configuration was an option for Short Term Changes and 3-2-1 strategy was also a plus.	• The short term changes seems to be addressing the high priority recommendation item on the rubric but this should be stated explicitly. • Even though speakers/slides avoided jargon well, I think certain sections (like the 'recover integrity' point of the strategy section) could have been more in depth and technical. • focus on $ for risks and costs • The proposal could have been strengthened by mentioning specific tools needed to support the plan/recommendations. The strategy could be strengthened by mentioning how it specifically addresses all risks that had been identified previously. • Plan should include more details such as staff, hardware, software needed and timelines. • Should list role of all team members. • Your listed risks are largely just impacts, which is only one part of the equation for risk. Your strategic plan is well thought out, but how does it reduce the risks you just talked about? Avoid jargon, like 3-2-1 backup strategy.

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	250	0	125	0	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
1220	207

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)
17	20	14	19	27	17	27	27	22	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
18087.80	40.20%

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
666

Green Team Survey Comments
• Everything looked good. • Positions for ObsidianRift and Abyssmal Pearl are available in the header, but their position does not match the rubric. • cant connect • website unable to load. Says 'This site can't be reached' • Site did not load • Could not reach website • This site can’t be reachedweb.blue0077.cfc.local refused to connect. • This site can’t be reached • Can't reach the website. • your site is unreachable! • "Hello Team 77 a couple things were missing on your website. There is no logo for the ObsidianRift and a logo for the Abyssal Pearl within the site navigation bar. The footer text is incorrect should state 18451 Convention Center Dr. Tinley Park, IL 60477 and yours states Somewhere in Illinois Earch, USA. When logging into the admin page there no 'blue@obsidianrift.oil' and 'green-admin@obsidianrift.oil' and those users should have admin tags and they do not. When clicking on the career webpage I get this error: BadMethodCallException Method App\Livewire\Pages\Careers::render does not exist." • This page isn’t working • The accent color in the middle of the website is yellow. The tag line capitalization is not exact; the words are there but not the proper capitalization. There are only 2 users, Red and Green users. The address is incorrect - it says 'https://blue.local, Somewhere in Illinois'. The website is missing the logos in the header. • company name misspelled, gold tint on image, internal service error careers page