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

KANSAS STATE UNIVERSITY

K-STATE CDC PURPLE

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 56 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	595	39.67%	20
Security Documentation	1210	96.80%	8
C-Suite Panel	1162	92.96%	7
Red Team	875	35.00%	44
Blue Team	1957	97.85%	6
Green Team Surveys	1358	90.53%	29
Deductions	0		
Overall	**7157**	**71.57%**	**29**

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	595

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

1	Yes	10.7	Yes	17	Yes
2	No	10.8	Yes	18	Yes
3	No	10.9	No	19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6	No	11.3	Yes	22	Yes
7	No	11.4	Yes	23	
8	No	11.5	Yes	24	
9	No	11.6	No	25	No
10.1	Yes	11.7	Yes	26	No
10.2	Yes	12		27.1	Yes
10.3	Yes	13		27.2	Yes
10.4	Yes	14	No	28	Yes
10.5	Yes	15	Yes	29	No
10.6	Yes	16	Yes	30	Yes

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	1210

Strong Points	*Areas of Improvement*
• Great job hitting the major points on the rubric. Tables and longer sections were formatted cleanly (e.g., using bold) for readability. • great job structuring your system hardening section • Covered great amount of details with clarity and looking good to present. Overall great effort by the team. • Great system overview!! It is at the appropriate level for the audience, and describes the system as a whole.	• One AD/DNS row listed with wrong IP. While you did a good job overall addressing a 'senior leadership' audience throughout, the vulnerabilities in particular could be better tailored to them. • show connections within network diagram • Asset inventory can be more readable to avoid certain bold highlighted rows (not sure the purpose of bold). • Very good hardening steps, but would like a little more justification for why you took each step to begin with.

Strong Points	Areas of Improvement
• Your report shows a good effort to document how the systems were secured and maintained. You identified realistic issues and included general security actions such as patching, enabling firewalls, and using antivirus tools. The document easy to follow even for someone without a deep technical background.	• Your hardening section would benefit from much more detail. It doesn't mention hostnames or IP addresses, which makes it difficult to connect your actions to specific systems. Consider including clear references for each host and explain what you did for each one (for example, "Web Server 10.0.0.5: disabled directory browsing, enforced HTTPS, updated Apache modules"). You also didn't include CVEs or specific vulnerabilities fixed, which are important for showing the real value of your hardening work.

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	1162

Strong Points	Areas of Improvement
• The presentation was very clean and professional. • Very good presentation, well presented and explained. Risks, Strategy and Recommendations. • The team started the presentation strongly with a good introduction, the video is approximately 5 minutes, time is used well, two team members presented and shared the time, and clearly acknowledge other team members who were not present. • Presenters clearly summarized the risks with notes to reputational impacts and distinct financial impacts in a manner that would be suitable for all C-suite executives. They recommended the appropriate number of high priority actions with sound reasoning for them and noted that there would be consequences for not taking action. Each high-priority action also has justification as to how they lesson identified risks and the proposed actions require a minimal level of additional funding. Their security strategy is well laid out and provides a complete approach that is a reasonable mix of policy, procedure, and technology that addresses the previously identified risks.	• I would have liked to see more specific details on the recommendations. what tools, software, and hardware will you implement? • Presentation could've been built to help better the explanation that was done. • Sam noted that they recommended implementing "open source software to improve monitoring and oversight of the network" in his presentation but this is not detailed on the slide. This is an extremely important recommendation, that can be done using open source software (per the rubric guidelines) but not documenting it as a separate recommendation in the high-priority recommendations slide is an oversight and implies this recommendation is less important than the others when this is not the case. • Nothing identified • Please specific about costs

Strong Points	*Areas of Improvement*
• Everything was presented well. The presentation looked professional. • Able to identify risk and solution	

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
125	0	125	125	0	125	125

Whack a Mole		
WAM1	WAM2	WAM3
0	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	482

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
42192.50	93.76%

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
1358

Green Team Survey Comments
• all is operational, the only thing of note is your footers! There is none on the front page and the other pages do not have the correct text.
• "The company name was listed twice in the footer on the main homepage.
• The rest looked good!"
• great job
• Address missing from footer on main page
• Your footers are all there, but make sure on the front page either a user can see the full text! Otherwise, you're doing great!
• Good job
• Website looks perfect, good job!!
• footer slightly cut off on homepage
• 5:42 This site can't be reached
• site cannot be reached