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

THE UNIVERSITY OF KANSAS

JAYHACKERS

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 54 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	1020	81.60%	55
C-Suite Panel	1123	89.84%	9
Red Team	1750	70.00%	8
Blue Team	1736	86.80%	47
Green Team Surveys	1298	86.53%	7
Deductions	0		
Overall	**7522**	**75.22%**	**7**

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		10.8	Yes	18	Yes
3		10.9	Yes	19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6	No	11.3	Yes	22	
7		11.4	Yes	23	
8		11.5	Yes	24	
9	No	11.6		25	
10.1	Yes	11.7	Yes	26	
10.2	Yes	12		27.1	Yes
10.3	Yes	13	Yes	27.2	Yes
10.4	Yes	14		28	Yes
10.5	Yes	15	Yes	29	No
10.6	No	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	1020

Strong Points	*Areas of Improvement*
• It definitely shows that the team put much effort into identifying vulnerabilities and listing mitigations. • "Good system overview, although I would have moved the last few sentences to the beginning of the paragraph. Put the high level holistic information first. • Vulnerability mitigations were appropriate for the audience, and your list was very thorough." • listed the asset and the vulnerabilities • Demonstrates a strong procedural framework for hardening and remediation	• The narrative in the System Overview seems hastily pulled together and uses a few acronyms that aren't described. There is lack of spacing and formatting that would be expected in a professional presentation to senior management and that would help with readability of the report. The asset inventory is limited. The network diagram does include all of the components and shows logical connections, also it provides a legend which is great, the overall problem is that the network diagram is almost unreadable with the font and dark

Strong Points	Areas of Improvement
using industry-standard tools and best practices. • Network diagram should be exported as am image then inserted into the document instead of include a screenshot that include the entire desktop.	background choice. Also it appears to be a screen shot of someone browser and desktop rather than just the network diagram. It would also be helpful if the network diagram had a title and simple one sentence description, again this is about professional presentation and readability for senior management. Finally, the System Hardening section is quite brief and while it covers most of the top level suggestions for basic system hardening, it could be more developed. • Network diagram, the way it is presented, is hard to read. • Hardening steps should be more comprehensive and explain why you took each step and what the benefit is. • Too much jargon is listed in the system overview/user definition, and the network diagram was too small to view; I had to expand it. No proper listing of the system hardening done • The vulnerability section could more clearly distinguish between completed mitigations and those still pending, giving a sharper picture of overall system readiness.

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	1123

Strong Points	Areas of Improvement
• Coherent framework integrating monitoring, maintenance, training, and backups; very professional tone. • Risks were covered well • The coverage on the various areas of financial risk was excellent, but needed some approx. potential cost values, fine levels or law suits based on previous events that are referenceable. Response strategy was also well worded for non technical /C Suite to start, but then doesn't use open source but free low usage commercial options that are likely to cost in this sort of environment, and how many pen tests a year at $15K each.	• Risk description could better emphasize business impact rather than primarily technical downtime. Video of presentation had too little contrast. • I would recommend not filming the projector. • Simplify cost of solution vs cost of not having the solution comparison by giving more specific (and realistic) details on the financials • The visual could be brighter. • The video of the presentation isn't the best quality, the slides are clean but would have been improved with either better quality video or the direct briefing.

Strong Points	*Areas of Improvement*
• This felt almost professional in the points and call to action and recommendations. • Clean, concise, professional briefing. • Rock-solid presentation, whole team contributed and I like how you even mention the insurance impact, everyone forgets about those premiums!	• Your monitoring & pentesting recommendations are great, would have been nice to see a little bit more on security controls

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	0	250	125	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
1425	311

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	23	26	27	26	21	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
27176.50	60.39%

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
1298

Green Team Survey Comments
• no footer on home page.
• footer not on main page
• No Footer on Home Page.
• Recommend putting the footer on the home page
• No footer on main page
• no footer text on homepage
• not all your accents are correctly colored, and you do not have a footer on your front page.
• Missing footer on home page.
• Good job but I recommend having footer on the home page like the others
• 5:42 This site can't be reached
• site cannot be reached