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

XAVIER UNIVERSITY

XCALIBER

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 97 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	477	31.80%	38
Security Documentation	843	67.44%	77
C-Suite Panel	967	77.36%	58
Red Team	750	30.00%	53
Blue Team	983	49.15%	90
Green Team Surveys	109	7.27%	86
Deductions	150		
Overall	**3979**	**39.79%**	**86**

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	477

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		19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6	No	11.3	No	22	
7	No	11.4		23	
8		11.5	Yes	24	No
9	No	11.6		25	
10.1	Yes	11.7		26	
10.2	Yes	12		27.1	No
10.3	Yes	13		27.2	
10.4	Yes	14		28	Yes
10.5	Yes	15	Yes	29	Yes
10.6	No	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	843

Strong Points	*Areas of Improvement*
• Covered great amount of details with clarity and looking good to present. Overall great effort by the team. • The network diagram had all the proper connections that would be needed that many skipped over. • You presented a thorough list of known vulnerabilities, and your system hardening section was laid out in a clear and organized way. The structure showed solid understanding and made your work easy to follow. • Clear and easy to read network diagram.	• System overview to be kept at executive level to understand the details. • The justification for the steps was there but it was not fully elaborated and more of a passing reasoning. • Including a brief mention of the tools you used during your scanning would strengthen the context behind your findings. Your approach is solid and the quality of your work shows real capability, adding that detail would elevate an already strong effort.

Strong Points	Areas of Improvement
	• The documentation could have used greater focus on the senior leadership audience. This includes defining acronyms, avoiding technical jargon, crafting easily read sentences, and using consistent formatting throughout.

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	967

Strong Points	Areas of Improvement
• Good presentation with strong detail on the identified risks and the strategy to reduce risks. • Risks were covered well • Able to identify risks and solution. I love the images. • Financial Impact Quantification: The presentation directly connected technical failures (ICS communication failure, gas compression malfunction) to specific financial consequences, such as calculating the potential revenue loss ($130,000 per day) and the direct loss during the 40-second outage ($90). This detailed financial analysis clearly showed the C-Suite how risks affect the company's bottom line, which is essential for this audience. • Regulatory and Reputational Risk: The team successfully highlighted external risks, specifically mentioning possible fines of up to $55,000 per day for failure to meet regulations and the risk of involvement by the EPA due to potential Clean Air Act violations. They also addressed reputational harm and loss of public/investor trust. • Complete Strategy and Recommendations: The team provided a complete security strategy, including three or more long-term action items (access control, human reliability training, third-party governance, and backup planning), meeting the Exemplary requirement for Strategy to Reduce Risks (30%). They also delivered four specific, high-priority actions (isolation, real-time log analysis, incident response	• Areas for improvement include the high-priority recommendations which could benefit from more detail regarding the additional funding and rationale if recommendations are not followed. Additionally, the solutions and training plan, which outlines three programs, should align with the long-term strategies and come prior to presenting the high-priority recommendations. This slide seemed a bit out of flow. It would have been ideal to include this information with your risk reduction strategies. • Recommendations are likely too low-level to be appropriate for executive interaction • Not all strategies were tied to identified risks • Provide the improvement of the financial impact of the company • Incorporate Visual Data: The query noted that the team used slides but lacked ""visual charts and calculations. For a briefing intended for the C-Suite, visual aids, slides, and other materials must have a consistent, professional appearance. Since the team quantified risks (e.g., $130,000 loss per day and $55,000 daily fines), displaying this financial data in a professional graph or chart would have been far more impactful than simply reading the numbers. Visualizing these critical impacts enhances the clarity for a non-technical C-Suite audience. • Strengthen Justification with ROI: While the recommendations were well-reasoned,

Strong Points	*Areas of Improvement*
checklist, and regular maintenance) with complete and consistent reasoning. The proposed solutions, such as implementing a security awareness training program and an incident playbook, also addressed staff communication and policy changes. • Business Risk Impact breakdown	explicitly linking the proposed high-priority actions to Return on Investment (ROI), cost, and timeline could strengthen the overall pitch. The Exemplary criteria require actions to use only free or open-source tools or require minimal funding. Explicitly stating the cost-effectiveness of implementing actions like log analysis or regular maintenance (which can be ""cheap"" but provide a ""high return"") would solidify the argument for the leadership team. • Optimize Presentation Delivery: Although the team met the requirements for having two active presenters and acknowledging all team members, presenting with two members sharing a single camera can sometimes lead to minor visual distractions or perceived inequality in participation, which can affect the Quality of Presentation score • practice delivery a bit more, I know in front of a camera is not easy though.

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	0	0	0	0	125

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
950	33

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)
15	16	0	0	17	8	26	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
2942.65	6.54%

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
109

Green Team Survey Comments
• Logos are in the header but they are not where they should be according to grading sheet.
• Website did not load.
• This site did not load. I tried it a couple of times and copied and pasted a couple of times. Just tried it again.
• Cant connect to site
• Page did not load. Error message: web.blue0097.cfc.local refused to connect.
• Your site is down!
• Could not connect.
• site could not be reached on multiple tries
• the page is not accessible
• website down 502 bad gateway
• Unable to load website
• site did not load
• Site is down (502 bad gateway error)

Green Team Survey Comments
• Website did not load. Error message: 502 Bad Gateway • The website doesn't load: 502 Bad Gateway. • bad gateway message • "502 Bad Gateway nginx" • internal server error • Internal Service Error • Hello Team 97 you site gives me an Internal Server Error. • 5:02 site is down Illuminate\Database\QueryException