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

UNIVERSITY OF CENTRAL FLORIDA

A TEAM WITH A DREAM

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 4 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	812	54.13%	5
Security Documentation	1112	88.96%	34
C-Suite Panel	1195	95.60%	3
Red Team	2000	80.00%	4
Blue Team	1681	84.05%	53
Green Team Surveys	1482	98.80%	4
Deductions	0		
Overall	**8282**	**82.82%**	**4**

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	812

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

1	Yes	10.7	Yes	17	Yes
2	Yes	10.8	Yes	18	Yes
3		10.9		19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6		11.3	Yes	22	Yes
7		11.4	Yes	23	Yes
8		11.5	Yes	24	
9		11.6	Yes	25	
10.1	Yes	11.7	Yes	26	
10.2	Yes	12	No	27.1	Yes
10.3	Yes	13	Yes	27.2	Yes
10.4	Yes	14		28	Yes
10.5	Yes	15	Yes	29	Yes
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	1112

Strong Points	*Areas of Improvement*
• The asset inventory and system hardening sections were well detailed. • Strong documentation on vulnerabilities and good hardening approach. • The team presented a solid and clearly written report that effectively covers key systems. The document's language is approachable, making it easy for non-technical readers to understand. The foundational structure is well thought out and sets a good base for future work. • Breakdown of multiple pieces of vulnerabilities.	• In the system overview, while the purpose of the system was clearly articulated, the language could be enhanced to better resonate with senior leadership. Additionally, providing a more detailed description of the scope would be beneficial. • The system overview lacked the quality the rest of the documentation had. • Vulnerability descriptions should be made more specific by including details such as the actual configuration values or settings that led to the finding.

Strong Points	*Areas of Improvement*
• The System Overview started the documentation strong. I liked the AWS networks and gateway along with the 2 VPNs in the Network Diagram. Overall the security documentation was strong and covered the requirements.	• Including severity ratings or prioritization for each issue would help readers focus on the most urgent concerns. • The diagram should also include a simple legend and system labels, and formatting across the report should remain consistent. • Vulnerabilities are too detailed for an executive audience. • Enhancements that could have improved the documentation include stronger business focus of the systems in the System Overview; Ensuring that the Asset Inventory and Network Diagram match, specifically MySQL was listed in the Network Diagram, but not the Asset Inventory. In the System Hardening the HMI and PLC systems should have vulnerabilities identified, but not be mitigated.

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	1195

Strong Points	*Areas of Improvement*
• Clear presentation of operational and business risks that includes financial impacts. Love the way you incorporated the visuals with the team presentation. Strategy included longer-term action items and addressed identified risks but was not comprehensive (how do these protect reputations, avoid lawsuits, etc.). Great work noting the upcoming regulations and using that to justify recommendations and other high priority actions. • Not only was this very clearly a collaborative effort across the team, but the overarching visual layout was captivating and professional. Rather than a slide deck, the text was minimal and reinforced with easy to comprehend icons. Truly well done presentation! • The video was professional with simple and easy to follow graphics. • Presentation was clean and professional, with delivery well balanced across team members. Risks were relevant, clearly	• Strategy included longer-term action items and addressed identified risks, but was not comprehensive (how do these protect reputations, avoid lawsuits, etc.). • The actual content was brilliantly conveyed, but the segue in speaker sometimes aligned with the shift in focus and visual, but other times the speaker would change as if halfway through an idea. Much like each paragraph should have a single central idea, I feel as if each speaker should align with a single focus and a single visual, and each of these should change together from one to the next. • Things were explained well and the rubric was followed. • Great job, just a few notes. Under risks, consider ordering by criticality (ex: address rig damage and loss of life first, emphasizing human and environmental safety as top-tier concerns). It would also help to visually prioritize the risk-mitigation strategies on the slide to guide the C-suite

Strong Points	*Areas of Improvement*
stated, and free of unnecessary technical jargon. It was effective to call out relevant regulations, financial impacts, and liabilities. Risk-reduction strategies were sensible in the short term, included some long-term actions, and aligned with the identified risks. High-priority recommendations were presented in a mostly non-technical, financially realistic manner. • Very professional presentation: Students were professionally dressed and spoke in a professional and articulate manner. Professional editing of video. Well researched and presented. • Impressive presentation editing and visuals with delivery appropriate for executives. Strategies identified clearly specify reduction of the identified risks including health/safety. Well-reasoned and well-delivered presentation.	with a clear timeline. Currently, two strategies are short-term (tactical: backups, temporary shutdown) and two are long-term (policy/strategic: asset inventory, incident response). Since executives tend to focus on strategic goals and may not be too concerned with tactical, try to focus on long-term, policy-based measures such as third-party vendor reviews or business continuity planning. • Reference list at the end of the presentation with further readings and list of related software recommendations would help give clear takeaways for the C-Suite to consider. Strategies to reduce risk are a little jargony and contain technical details without explain for non experts, such as clean-backups, logging with Elastic. More details or higher level details would be helpful for non technical C-Suite members. Open source software may be free, but costs from equipment and personnel should still be calculated and included. Yes, these measures will be less expensive than a breach, however, the C-Suite will want more specifics . • No points were deducted, but some of the presentation felt rigid and overly scripted.

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	250	125	125	250	250	250

Whack a Mole		
WAM1	WAM2	WAM3
250	125	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
1480	201

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	27	27	27	27	27	26	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
17586.45	39.08%

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
1482

Green Team Survey Comments
• Great Job! • On the Admin: User Management page, there is no 'Admin' tags. It only says 'Yes' or 'No.' • On the admin page, the name should be Green User and Green Admin, not Green Team 01 and Green Team 02. • Excellent job Team 4! • Slight variation of template however, meets all criteria • slight variation • Very nice!