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

UNIVERSITY OF CENTRAL FLORIDA

TINLEY PARK MENTAL HEALTH CENTER

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 89 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	917	61.13%	2
Security Documentation	1212	96.96%	7
C-Suite Panel	1118	89.44%	11
Red Team	2125	85.00%	2
Blue Team	1957	97.85%	6
Green Team Surveys	1454	96.93%	1
Deductions	0		
Overall	**8783**	**87.83%**	**1**

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	917

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	Yes	10.9	Yes	19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	Yes
6		11.3	Yes	22	
7	No	11.4	Yes	23	No
8		11.5	Yes	24	Yes
9	No	11.6	Yes	25	No
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	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	1212

Strong Points	*Areas of Improvement*
• There are so many strong points for this submission, it's difficult to list just one. The network diagram is great, includes the logical connections between components on the network and a legend for readability. The System Overview is a well written, bottom line up front representation of the current state of the network at the site. The Asset List is extensive, as is the list of Vulnerabilities and Mitigations and it contains useful, critical information. The System Hardening is very thorough and well organized, especially helpful that it includes	• Overall this is an excellent submission and really well organized for a professional presentation to senior management. I don't have any suggested improvements, just a question really about the choice to not include HMI and PLC in system hardening. It makes sense from a digital forensics it makes sense to hold those systems and do any mitigations, but from the safety and security of the site perspective that the senior management probably prioritizes: why not take a forensic digital copy of the disk for each system, using something like

Strong Points	Areas of Improvement
the tools used to accomplish the investigation and recommendations. • Good catch on the logical connections in your network diagram. Overall excellent submission. • Appropriate level of detail in vulnerability listings. • The report was solid in terms of content, the formatting was simple and effective. • Everything was perfect, congrats!	Autopsy, and then move the copy to a sandbox for further investigation. This would allow these critical systems to also be included in system hardening. • Good tasks in hardening, but were there phases? • Several hardening steps listed were actually remediation. • The network diagram could have been clearer, there was a confusing intro "note" in the vulnerabilities section. • More attention (Mitigation of vulnerabilities in HMI and PLC is not allowed).

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	1118

Strong Points	Areas of Improvement
• I appreciated how many team members presented in the video and how well rehearsed, and professionally dressed, each of them was. • Nice Job. I like how you mentioned that some of your recommendations are simple system setting configurations. • The team had great statistics regarding the impacts of training and free resources to provide the training. There is a very strong call to action that references the consequences of choosing to ignore the recommendations. The high priority action items were technologically adapted and advanced but were presented in a manner that would be understood by an executive. • Great use of a real world example that is within the same industry! This really helps the c-suite understand the potential cost and reputation damages that can occur. • Moving on from one point to another in a logical manner, accentuating the key information. • Great way to do the presentation. It was unique and still well suited to address the c-suite. • Very professional.	• The risk management strategy could have been better tied to identified risks. Also, some of the high priority actions had cost involved and quantifying this cost with specific figures for the c-suite is important. • The physical security overhaul, while potentially important, would be extremely expensive and time intensive and not an appropriate high priority action given the context of the scenario as the contractor was conducting approved maintenance in an area they reasonable were supposed to have access to. The team's recommendation of establishing an asset inventory and auditing process would, theoretically, catch the introduction of new/unknown equipment that an insider threat may attempt to introduce making this risk management strategy more important than a physical security overhaul. • It would have been good to hear about some long term recommendations that touch on network policies, intrusion detection systems, hardening of systems, etc. and how those could support a long term security posture. • I recommend continuing using real world examples from the same domain, but look

Strong Points	Areas of Improvement
	for cyber specific attacks to further pull the c-suite towards the goal you want. Great job! • More visual elements to captivate the audience and more passion. Maybe a final 'call to action' to guide on what to do next, or specific actions toward goals. • Ensure that the strategy to reduce the risks directly correlate with said risks mentioned and are not just generalized. • You need to talk about how your mitigations directly relate to your aforementioned risks.

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	250	250	250	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
1480	477

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	26	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
41737.41	92.75%

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
1454

Green Team Survey Comments
• Careers link does not work when I checked. Colors did not match the required template. The navigation buttons/links did not work. • Good job! • Excellent work! • users added • Great job! You secured that oil rig so tight even the crude couldn't slip past you! • The User Management section has 2 extra users called Muhammad & Muhamamd2. Otherwise, everything else is good to go!