



UNIVERSITY OF SOUTH FLORIDA

USF CYBERHERD

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 93 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	911	60.73%	3
Security Documentation	1156	92.48%	20
C-Suite Panel	1023	81.84%	43
Red Team	875	35.00%	44
Blue Team	1922	96.10%	15
Green Team Surveys	1460	97.33%	18
Deductions	0		
Overall	7347	73.47%	18

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	911
----------------------	------------

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	
6		11.3	Yes	22	Yes
7	No	11.4	Yes	23	Yes
8	No	11.5	Yes	24	
9	Yes	11.6	Yes	25	Yes
10.1	Yes	11.7	Yes	26	
10.2	Yes	12	No	27.1	Yes
10.3	Yes	13	No	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	1156
-------------------------------------	-------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> Detailed, well-organized, and persuasive The vulnerability and hardening sections show excellent attention to detail and demonstrate strong teamwork and technical execution. Great system overview and thorough asset inventory. Love the color-coded severity on the vulnerabilities list. Appreciated all the details added to the network diagram. Everything in this presentation was a strong point. Congratulations on your performance, keep growing! 	<ul style="list-style-type: none"> Could condense slightly to improve executive readability A short executive summary or key highlights section at the start would make it easier for leadership to quickly understand the team's results. Network diagram is too detailed. Typically, don't need to list open ports on a network diagram. A functional label for each node is fine. The system hardening should not be a diary, but a list of steps, with justification, taken to harden each system. These should be

<i>Strong Points</i>	<i>Areas of Improvement</i>
	<p>written in a way that is repeatable in the future.</p> <ul style="list-style-type: none"> • System hardening is supposed to be focused on overarching ideas and not all specific steps taken. Also, it should have proper justification for each of these steps. • No need for improvement, it's perfect.

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	1023
----------------------------	------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> • Speakers were well-rehearsed and slides well-designed. In particular, keeping words briefer on the slides helps the listener focus on the speaker's words. • Addressed impact of transparency in relationships with partners. • Able to nail the risks and solution • Nice overview of strategy summary • high level business talk about service without the need to go into technical detail. and low cost long term plans. 	<ul style="list-style-type: none"> • Quantifying the risks helps the c-suite understand the importance of taking action. For instance, discussing how much money could be lost with production disruption is important. • More detail could be given on the high priority actions section in particular, and relating these more thoroughly to the risks. • In acknowledging contributors, don't use last names (for your privacy). • Long-term recommendations don't clearly tie back to risks • First, make sure you are addressing the team members as well. Second, Please be provide a bit of information on the presentation instead of just a list. Third, provide the improvement of the financial improvement after implement C-Suite to the company! • More emphasis of future risks and financial impact of risks related to ops/business • Conclusion was too generic, after already having had the long term recommendations

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	250	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
1475	447

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
39064.85	86.81%

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
1460

Green Team Survey Comments

- logos in the wrong position but still there
- Good Job.
- The logos locations were different from the example but it's listed so I didn't deduct the point.
- logos are not surrounding the company name like in original
- "This one is almost perfect — the header logos do not match the template [the main page is scrollable with footer, most I review are not] The logos should be alongside obsidianriftenergyco on both sides not alongside oil rig status and sign up per the template. Their placement is off."