



COLLEGE OF COASTAL GEORGIA

HAIL THE SAIL!!!

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 48 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	379	25.27%	60
Security Documentation	1244	99.52%	1
C-Suite Panel	1088	87.04%	23
Red Team	250	10.00%	82
Blue Team	1445	72.25%	75
Green Team Surveys	1369	91.27%	61
Deductions	0		
Overall	5775	57.75%	61

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	379
----------------------	------------

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

1	Yes
2	
3	
4	No
5	Yes
6	
7	
8	
9	No
10.1	Yes
10.2	Yes
10.3	
10.4	Yes
10.5	Yes
10.6	No

10.7	
10.8	
10.9	
11.1	Yes
11.2	Yes
11.3	Yes
11.4	
11.5	
11.6	
11.7	
12	
13	
14	
15	Yes
16	Yes

17	Yes
18	Yes
19	Yes
20	Yes
21	
22	
23	
24	
25	Yes
26	
27.1	No
27.2	No
28	Yes
29	
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	1244
-------------------------------------	-------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> • Thorough list of vulnerabilities. Good documentation of system hardening with justification • Your document is well written and easy to follow. The vulnerability list is detailed and organized by host, and it makes it simple to track your work. Your technical explanations are good. It is clear your team understands both IT and OT environments. • Very good and strong document • system overview and hardening sections were very thorough 	<ul style="list-style-type: none"> • Use caution in differentiating mitigation and hardening steps. • Adding a short executive summary for the "Hardening" section with your top risks and outcomes would make the document easier for a non-technical reader. • Could focus more on business/operational than in component descriptions. • Network diagram had the switch exposed

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	1088
---------------------	------

Strong Points	Areas of Improvement
<ul style="list-style-type: none">The use of the time was good and team looks professionalGood detail on high-priority recommendationsThe information was presented well.all of it. Risk to core business was excellent, referencing a \$400M+ fine for a competitor previously for something similar will get attention. Impact to different systems was comprehensive. In addition to the strong Recommendations justifications, I also liked their proposed solution, although can't score more for that.Clean and professional slides are easy to read and support talking points well.Good presentation with a clear demonstration of the tools and orchestration processes used for remediation. The team effectively connected technical actions to the overall mitigation strategy.	<ul style="list-style-type: none">Presentation presented a typo. Risk were presented in isolation, strategy and recommendations were not directly related to the risks to understand the strategy.Although the recommendations and strategy are good practices, they aren't clearly tied back to the risks or incident.Not all mentioned risks were directly addressed later on.a very slight bit of polish, and felt the summarization at then end went on a bit; but it was good to re-cover the key points.The presentation felt a little rigid - like reading from a script (no points deducted). The presented risks tied to business impact very well. Strategies could be stronger but fulfilled the rubric.Great work overall, keep building on this foundation by continuing to develop your confidence and professional communication as you refine your technical skills.

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	0	0	0	0	125

Whack a Mole		
WAM1	WAM2	WAM3
0	0	0

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
1445	0

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	21

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
0.00	0.00%

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
1369

Green Team Survey Comments

- logo is too small. there's no management button.
- logos in navigation bar are in the wrong location
- No footer on a home page
- The logo is not in the required position. Too small to see.
- no footer on Sign Up page, other than that, the site looks great!
- Logo exists but way too small
- You do have the logos but heads up they are hard to see and they are located differently from documentation so you might want to adjust that.

Green Team Survey Comments

- Logos are in wrong location on navigation bar
- Logo hard to see but did see them might want to fix that
- Good job! Your rig shows 'Not Operational' within the status and you are also missing your logos within the header.
- Really hard to see the logos
- logos are tiny and in the wrong location
- 5:52 This site can't be reached