



## UNIVERSITY OF TAMPA

### CYBER SPARTANS

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 24 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	397	26.47%	56
Security Documentation	878	70.24%	76
C-Suite Panel	1065	85.20%	30
Red Team	750	30.00%	53
Blue Team	1330	66.50%	84
Green Team Surveys	120	8.00%	80
Deductions	0		
Overall	4540	45.40%	80

## 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.

<b>Anomaly Score</b>	397
----------------------	-----

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

1	Yes	10.7		17	Yes
2	No	10.8		18	Yes
3	No	10.9		19	Yes
4	Yes	11.1		20	Yes
5	Yes	11.2		21	
6	No	11.3		22	
7	No	11.4		23	
8	No	11.5		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	No
10.4	Yes	14	No	28	No
10.5		15	Yes	29	
10.6		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.

<b>Security Documentation Score</b>	878
-------------------------------------	-----

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> <li>Good system overview. Network diagram is very clean. Hardening plan looks good.</li> <li>Good list of vulnerabilities and mitigations. Even though scored low due to quantity and some errors, the few you have are written well.</li> <li>Super well-organized and practical with clear logic.</li> <li>The system overview did a good job of describing the operational importance of the system. This is important when speaking to leadership.</li> <li>Very complete and clear documentation.</li> </ul>	<ul style="list-style-type: none"> <li>Network diagram missing IP for task box, and router is outside of subnet. Vulnerability listing had different fonts; CVEs not listed by name; less than 23 of build vulns. Hardening plan lacks paragraph spacing; underlining or bold would have helped reader focus on particular issues.</li> <li>System overview is missing information about multiple systems. Task Box IP missing from network diagram. Not supposed to mitigate PLC. System Hardening section format is difficult to read and looks unorganized, suggest technical editing.</li> </ul>

<i>Strong Points</i>	<i>Areas of Improvement</i>
	<ul style="list-style-type: none"> <li>• Might've been even better with a short executive summary of risks.</li> <li>• The document could have used some more polish: double check network diagram IP addresses, remove unused rows from tables, and more clearly justify actions.</li> <li>• The executive level framing could be improve a little bit more, but is still very good</li> </ul>

### 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.

<b>C-Suite Panel Score</b>	1065
----------------------------	------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> <li>• Entire team present for briefing. Good listing of 3 risks. Immediate isolation - not a given. Great choice. You named several tools but didn't emphasize their cost or compatibility with the company's IT network. Provided several apps to use along with their cost.</li> <li>• I believe that this might have been the very best synthesized presentation that I have seen, so many other teams just offer everything in the assigned order from incident to related risks to strategy to recommendations, but this is the first team that I encountered that again and again kept relating how each item intersects with the others, clearly laying out how this recommendation helps address this risk and could have mitigated this part of the incident. The overarching cohesiveness of the verbal presentation here was truly impressive!</li> <li>• Good sharing of presentation time and providing details</li> <li>• Good analysis of risks.</li> <li>• Very good organization and good call to action.</li> </ul>	<ul style="list-style-type: none"> <li>• Lack of slides negatively affected impact to C-Suite. Allow team to wave their hand when you introduce them. Initial speaker should slow down the pace - too fast. Use slides - give C-Suite something to follow along with. C-Suite would have to take notes based on your verbal presentation. 2nd speaker was too quiet. Calculate the estimated cost for one day loss of production (2,000 barrels) and state that for the C-Suite to consider. Don't chew gum - member on far left :) Don't end on a negative note. Instead, use "By agreeing to our recommendations, (restate them), the company (good things) and avoid (bad things).</li> <li>• This presentation was profoundly hurt by a lack of any semblance of a visual. The entire presentation is six people gathered around a table taking turns reading from some off camera script. Because there were no slides or edits or visuals in any way, the focus was entirely on the readers, so each persons' nervous monotone voice as they read became the focus. The most exciting part visually was when someone just outside this room walked by the window behind this group. While it didn't have to be a slide deck per se, some visual or filmic edit would have broken it up. And if that truly was not an option, then each person could memorize their parts and spoke directly to the camera,</li> </ul>

Strong Points	Areas of Improvement
	<p>one at a time so that they connected with us in the audience as one human to another.</p> <ul style="list-style-type: none"> <li>• Lots of distracting unprofessionalism. Slow down. Lack of visual aids, which are necessary to help C-suite to focus. Strategy does not directly relate to identified risks</li> <li>• Tough to follow along with no visuals. Suggest sharing your slide deck with key points that the C-Suite can focus on.</li> <li>• Lack of visual aides was distracting. Some strategies and high-priority recommendations were duplicative, not additive, and didn't tie back to presented risks in a way that communicated how they might have prevented this incident.</li> <li>• Too technical. There is no need to dive into all the different options of Open software.</li> </ul>

## 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
0	0	0	0	0	125	125

Whack a Mole		
WAM1	WAM2	WAM3
125	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
1330	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)
22	23	27	26	27	19	22	27	22	27	24

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
120

### Green Team Survey Comments

- When opening the website, the user is met with an internal service error. The website does not even open or operate.
- Database file at path [/var/www/html/database/database.sqlite] does not exist. Ensure this is an absolute path to the database. (Connection: sqlite, SQL: select \* from 'sessions' where 'id' = 4iPk9pjoFzQhWNaDUQyulNpGRe1ZLk4rmeJB1IAf limit 1)
- Website not loading.
- site did not load
- Faced Internal server error - Database file at path [/var/www/html/database/database.sqlite] does not exist. Ensure this is an absolute path to the database. (Connection: sqlite, SQL: select \* from 'sessions' where 'id' = NRAcYtetNoX9FFrLOJd43SNN4cQRxFJiK9H7cNgz limit 1)
- "Internal Server Error Illuminate\Database\QueryException Database file at path [/var/www/html/database/database.sqlite] does not exist. Ensure this is an absolute path to the database. (Connection: sqlite, SQL: select \* from 'sessions' where 'id' = K9COXbr3ynqKRY1m5ttKclzhHkdXBnPulgBMFtQf limit 1)"
- Internal Server Error. Will not load website.
- site does not load
- Unable to login.
- No login button
- The required colors were not followed. The navigation bar is missing login button/link. No background image. Incorrect tag line. No career options/lists. No login options. No footer on the homepage. The rig status link returns with internal server error. No logos.

### *Green Team Survey Comments*

- wrong color, incorrect header info, wrong image and tagline, no job opening options, cannot log in, wrong footer info, rig status page does not load, no logos in header
- Only half of the website loads. There is no functionality and the user is not able to actually engage with any of the website's elements.
- Your web server appears to be compromised or not configured properly.
- Your site has been attacked. You don't have the appropriate accent color. Your header tags are in the middle of the page and out of order. You don't have the appropriate careers listed within the career page. It was difficult to find the login button due to being in the middle of page and covered by the logos which are in the middle of the page. I was unable to login as a user and a admin. There is no footer text at the bottom of the website, and I am unable to access the rig status page. Your logos are present but not within the header and covering the main picture in the middle of the website.
- 5:46 This site cant be reached
- Site is down