



## THE UNIVERSITY OF TENNESSEE AT CHATTANOOGA

### MOCSEC CYBER SECURITY

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 61 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	391	26.07%	57
Security Documentation	671	53.68%	91
C-Suite Panel	976	78.08%	52
Red Team	250	10.00%	82
Blue Team	1843	92.15%	31
Green Team Surveys	1009	67.27%	78
<i>Deductions</i>	0		
Overall	5140	51.40%	78

## 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>	<b>391</b>
----------------------	------------

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

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

<b>Security Documentation Score</b>	<b>671</b>
-------------------------------------	------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> <li>• Provided good detail within the asset inventory section. Good work!</li> <li>• Really strong start with the asset inventory and system overview. Shining point of this entry is definitely the network diagram. It's awesome to see the breakdown of system services along with the topology.</li> <li>• Good job on the asset inventory</li> <li>• Asset inventory were listed as well as their attributes</li> <li>• The team's vulnerability documentation is detailed and accurate, showing deep understanding of the systems assessed.</li> </ul>	<ul style="list-style-type: none"> <li>• Overall, the document could improve with more technical detail and clearer explanations. Additionally, the network diagram could improve by including critical components, such as the gateway router and links. Lastly, a more comprehensive list of vulnerabilities could improve the assessment significantly.</li> <li>• More time could have been dedicated to identification of vulnerabilities. It looked like this section was started but not finished. It'd also be good to give a higher level strategic</li> </ul>

<i>Strong Points</i>	<i>Areas of Improvement</i>
<p>Their tables are well organized and easy to interpret. The overall tone and presentation are professional and clear.</p>	<p>approach and justification in plain language for the hardening section.</p> <ul style="list-style-type: none"> <li>• In the System Overview, what does the system itself do? What is the sum of its parts?</li> <li>• Network diagram has WAY too much information. No need to have an icon for every open service on every machine. Machine type and IP and connections are sufficient for a network diagram.</li> <li>• More vulnerabilities found should have been documented. Also for next time the network diagram could be kept simple</li> <li>• Duplicate vulnerabilities were found under both the Web and Task servers and should be consolidated under the correct system.</li> <li>• Adding risk severity levels would strengthen the report.</li> <li>• Including a legend and labels in the network diagram would improve readability.</li> <li>• The team could also summarize unresolved issues and add short explanations for each major hardening decision.</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>	<b>976</b>
----------------------------	------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> <li>• Strong presentation, well explained the topics.</li> <li>• Loved that you included cost of oil to calculate losses!</li> <li>• Presentation was generally well-rounded and presented a number of good points. Strong contribution for this entry was definitely high-priority recommendations and ensuring to leverage changes and implementations that are low-cost and account for physical security as well as cyber. Another good point of coverage was financial impacts aligned with risks.</li> <li>• Good work in including a chart.</li> <li>• The graphics for Risk Reduction and Recommendations had good graphics.</li> </ul>	<ul style="list-style-type: none"> <li>• Strategy and recommendations were not directly explained and related to solve the risks initially presented.</li> <li>• Your risks were great, but you didn't follow through and highlight how your strategy or high priority recommendations tied to those risks.</li> <li>• Risk reduction strategy contained mix of short-term tactical and few longer-term policy changes. It would be good to focus more on the long-term strategic policies that the C-Suite can push as a part of organizational change. Also, a good chunk of the presentation was spent on the incident recap, it would be potentially better to make this a bit more concise so you can spend more time on your risks, strategies, and recommendations.</li> </ul>

Strong Points	Areas of Improvement
	<ul style="list-style-type: none"> <li>• Would recommend standing up when presenting to present as more active and engaged.</li> <li>• Security incident overview very technical and may be above the level of the c-suite.</li> <li>• Sound would have higher quality of speakers spoke closer to the camera/microphone.</li> <li>• Risk reduction strategy, timeline, cost, software and hardware requirements? Do staff need training?</li> <li>• Which free tools would be used?</li> <li>• Recommendations: includes jargon and acronyms C-Suite members not IT experts will be unfamiliar with.</li> <li>• I recommend have 1 student hold and control the camera and filming one student at a time speaking.</li> <li>• Font on graphics and chart is too small to read.</li> <li>• Separating the names into Presenters/Contributors would've made it easier to tell who was talking. Some of the charts had very small fonts, making them hard to read.</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
125	0	0	0	125	0	0

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
1475	368

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
32212.37	71.58%

## 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
1009

### Green Team Survey Comments

- No tabs on navigation bar
- check your navigation bar, logos, admins, and footer!
- after sign up, there is other selection button that doesn't take anywhere. color looks different. there's no 'user management ' button when log in.
- User management users and admin tags not there. Footer text format.
- The work 'Rift' is missing. The Admin > User Management is incomplete. The homepage does not have a footer. The logo is not in the required position.
- Blue and Green Admin not showing up in user management. URL in footer text
- The company name in the header is wrong. No admins listed on the admin page. The footer is not correct. You should not have a website link in it. The logos are outside of the navigation bar.
- Fix the logo placement in the header

### *Green Team Survey Comments*

- company name misspelled, URL in footer, green and blue admins not listed in user management
- Footer is messed up and logos are wrong. wrong domain added to footer. No admins. Admin button present
- Your footer information is incorrect, the proper users are missing when login as admin and your header is not setup right
- The company name is wrong, the logos are in the wrong spot and the users that should appear when in admin are not appearing.
- Hello Team 61 when logging into the admin page users 'blue@obsidianrift.oil' and 'green-admin@obsidianrift.oil' should have the admin tags, and there was none.
- your admins are gone, there is an extra link in your footers, and your logos are in the incorrect place.
- company name misspelled, blue and green admin missing from user management, URL in footer
- web.blue0061.cfc.local refused to connect.
- 5:52 This site can't be reached