



COLLEGE OF DUPAGE

CHEN'S ULTIMATE DEFENSE

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 15 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	174	11.60%	89
Security Documentation	1117	89.36%	31
C-Suite Panel	1019	81.52%	44
Red Team	250	10.00%	82
Blue Team	1506	75.30%	64
Green Team Surveys	1340	89.33%	74
Deductions	150		
Overall	5256	52.56%	74

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	174
----------------------	------------

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

1	No	10.7		17	Yes
2		10.8		18	Yes
3		10.9		19	Yes
4		11.1		20	
5		11.2		21	
6		11.3		22	
7		11.4		23	
8		11.5		24	
9		11.6		25	
10.1		11.7		26	
10.2		12		27.1	No
10.3		13		27.2	Yes
10.4		14		28	
10.5		15	Yes	29	
10.6		16	No	30	

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	1117
-------------------------------------	-------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> • Good system hardening write up. • Your documentation included a complete, clearly labeled network diagram. • All vulnerabilities were identified and fixed for every system. • Security controls were justified and matched business needs. • System hardening and framework were great. • Well crafted with Asset well listed • Excellent system description. 	<ul style="list-style-type: none"> • The network diagram had AD at the root where I would've expected to see a router that connected the local systems with the larger internet. • Make the asset inventory table easier to read and summarize details. • Use shorter paragraphs and headers for better document organization. • Polish formatting for a more professional look. • The network diagram could have had some more detail.

<i>Strong Points</i>	<i>Areas of Improvement</i>
	<ul style="list-style-type: none"> The network diagram not well completed, plus documentation pages should look more aesthetic Black font on blue background is unreadable :(Missing router & Internet on system diagram, subnet is improper (no x in IP address). Missing majority of vulnerabilities. Center network diagram on paper, avoid black background on system diagram.

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	1019
----------------------------	------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> Great presentation! You had strong details on effective strategies to reduce business risks. Fantastic job overall! The depth and knowledgeable insights in this presentation are profound. It is clear that those involved deeply understand the underlying issue here. The speakers and slide deck reference many nuanced specifics that underscored their solid understanding of the underlying issue. Truly well done on this aspect! I like how you mention the risk that would impact the financial stability of the company! Good work in providing specific job roles and work duties to the other team members. Both speakers communicate very clearly and professionally. Clear explanations of risk. Good job including the concerns of the C-Suite in impacts. Great approach to strategy. They are high level and directed to the cause of the incident. Try to make that connection to risks stronger, though. Presentation was suitable for all C-Suite members and coherent in terms of content. 	<ul style="list-style-type: none"> An area for improvement would be to provide additional detail for the high-priority recommendations, particularly on how they reduce identified risks. Instead of a general statement about minimal funding, clarify how this conclusion was reached and demonstrate that each recommendation requires only minimal additional funding. I felt that there was a lot implied between the problems offered and the solutions proposed and very much wish that these were far more explicit. However, the biggest issue was in the presentation itself. First and foremost, not being able to see any of the speakers distanced the audience from this team. They were just two ephemeral voices without any faces or bodies to connect to. As such, the entire focus was on the slide deck, and although the deck itself was clearly professional, it had two major issues: First, this deck was vastly text heavy. So much of this could have been so much more elegantly conveyed with images and icons rather than just filling a page with words. Second, the color contrast was deeply problematic as the text was different shades of blues and greens (and white) on a blue-green background. This reached a watershed moment when on the slide "Four Urgent Stabilization Steps (3-4)," the green text "Minimal funding - Maximum protection"

Strong Points	Areas of Improvement
	<p>is nearly illegible. If you let us see you, the presenters, then we could have something else to focus on than the concerns in this deck.</p> <ul style="list-style-type: none"> The only thing that would need to improve is that please turn your cameras on and speak more clearly through out the presentation May be beneficial to include a references slide and examples of recommended hardware, and software. You covered impacts of the current incident, but not overall risk of the current security posture. Remember that risk is calculated by both impact and probability, not just impact. Avoid jargon on the urgent steps, and provide cost estimates. What are the labor costs? How long will it take? How do they reduce the risks? Equipment damage as a business risk with financial consequences that could have been considered. Tying reputational damage with a financial impact would have also helped keeping consistency in risk depiction. Strategy doesn't adequately cover rebuilding compromised systems and the recommendations are disparate, and may not be feasible if the intent is urgent stabilization.

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	0	0

Whack a Mole		
WAM1	WAM2	WAM3
125	125	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	61

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	20	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
5361.89	11.92%

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
1340

Green Team Survey Comments

- web address in footer
- extra URL in footer
- footer text includes URL, header logos wrong position
- logos are flipped per example
- The footer text does not read as advertised.
- URL in footer
- The footer text has an extra URL.
- The logos are not in the required position.

Green Team Survey Comments

- incorrect footer
- footer text format wrong
- URL in footer
- Good work! For your color way it looks more reddish rather than a burgundy color. Your logos are present, but they are flipped compared to the reference images I have to check.
- URL in footer text, logos swapped positions
- Rock-solid work! Even Obsidian Rift's rigs approved Unfortunately, you're missing the footer on the login and signup pages, the rig-status page doesn't appear to load, and your logos in the navbar are reversed.
- Rig Status takes forever to not load
- Site is down