



JOLIET JUNIOR COLLEGE

CYBER WOLVES

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 25 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	219	14.60%	87
Security Documentation	895	71.60%	74
C-Suite Panel	937	74.96%	63
Red Team	875	35.00%	44
Blue Team	1855	92.75%	29
Green Team Surveys	709	47.27%	69
Deductions	0		
Overall	5490	54.90%	69

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	219
----------------------	------------

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	Yes
5	No	11.2		21	
6		11.3		22	
7	No	11.4		23	
8		11.5		24	No
9		11.6		25	
10.1		11.7		26	
10.2		12		27.1	
10.3		13		27.2	
10.4		14		28	No
10.5		15	Yes	29	
10.6		16	Yes	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	895
-------------------------------------	------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> • Very well written system overview, capturing the key purpose of each system appropriately for the C-suite audience. • The team did well in their review of the system and in their system hardening strategy. The network diagram was well-structured and clear to understand. • Great diagram, I really like the way you illustrated the open ports and how the webserver interacts with its services • Very good diagram. 	<ul style="list-style-type: none"> • Some minor omissions on asset inventory, but not enough to lose points. Network diagram small text and harsh colors are hard to read, and incorrect IP address. • "Some key services were not documented in the asset inventory, • Several vulnerabilities were not documented. • The system hardening section was overly technical for a C-Suite audience." • The system hardening section was a bit of a word salad; I'd like to see it cleaner with more details on log forwarding & analysis

Strong Points	Areas of Improvement
	<ul style="list-style-type: none"> Vuln list was a bit short.

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	937
---------------------	-----

Strong Points	Areas of Improvement
<ul style="list-style-type: none"> Very professional and good well rounded ideas to respond to the incident Great job showing how one down day costs more than the implementation of your recommendations. Able to identify the risk Strategy mentioned looks complete and clear. Great including video of the team and visuals as part of the presentation. Very professional. Slide deck was easy to follow and visible. Zero Trust framework and mentioned vendor compliance and security training for Human firewall. ICS incident response playbook was a great mention. 	<ul style="list-style-type: none"> Too much focus on the incident itself. Risks are not directly related to business/operational risks or are minimally mentioned. Strategies do not tie back to these risks. Be sure to proof your ppt, there was font on slides very similar to the background, I found myself trying to figure out what it said which takes away from what you are saying. Note: Should mention I am color blind and this wouldn't be the first time I thought colors are too similar but in reality it was clearly different colors to normal eyed folk. Tell us specific about the improvement when it comes to impact of the company financial changes The risk discussion does not adequately tie into financial impact. Recommendations most certainly require additional funding. The presentation template was a little busy and could have been simplified.

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
250	0	0	0	125	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
1445	410

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	25	27	21	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
35869.26	79.71%

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
709

Green Team Survey Comments

- The error 'the site can't be reached' at the time of evaluation.
- missing footer text on home screen
- Accent colors are orange, not maroon. No footer on the home page.
- too much of accent color, no homepage, red admin
- I couldn't open the page. The error message was 'This site cant be reached.'

Green Team Survey Comments

- Was in the middle of reviewing the website, then the site couldn't be reached anymore. Unable to check the login and oil-rig status.
- site not loading
- Website did not load.
- red admin
- not loading
- 'red' admin
- site inaccessible
- Site is down
- Hello Team 25 I was unable to access the site, I get an error stating that the site cannot be reached
- Address footer is supposed to be on every web page, but it's not found on the home.
- Main page replaced with cat and color changes
- no footer on homepage
- no homepage footer, 'Red' admin user
- Footer not on every page
- "website down
- "This site cant be reached web.blue0025.cfc.local took too long to respond. Try: Checking the connection Checking the proxy and the firewall Running Windows Network Diagnostics
ERR_CONNECTION_TIMED_OUT"
- Site is down