



UNIVERSITY OF ILLINOIS CHICAGO

0X636C61790A

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 73 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	461	30.73%	41
Security Documentation	956	76.48%	67
C-Suite Panel	951	76.08%	61
Red Team	875	35.00%	44
Blue Team	1697	84.85%	51
Green Team Surveys	250	16.67%	76
Deductions	0		
Overall	5190	51.90%	76

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	461
----------------------	-----

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	No	10.9	Yes	19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6		11.3	Yes	22	Yes
7	No	11.4	No	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	No
10.4	Yes	14		28	No
10.5	Yes	15	Yes	29	
10.6	No	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.

Security Documentation Score	956
-------------------------------------	-----

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> Technical depth and accuracy were present, along with appropriate use of tools. The team's diagram is neatly drawn and provides a good visual overview. Their narrative is clear, concise, and well suited for both technical and non-technical audiences. The structure and formatting are professional and easy to navigate. System hardening info was very easy to follow and well thought out. All of your sections were well thought out and developed. 	<ul style="list-style-type: none"> Organization of the document, using numbered lists or application of a pseudo color scheme to help senior management make informed decisions. Consider the need for quickly identifying the most important information is seconds. Rarely can this be accomplished using only plaintext. Asset inventory has question marks for services. The system overview only addressed the machines that made up the system, it didn't identify the overall system or its purpose.

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> • Good job with vulnerabilities and clear mitigations. 	<ul style="list-style-type: none"> • Your formatting needed some work. Use page breaks to separate sections. Also if you are going to use shading in a table, it should be used to separate sections or highlight certain aspects, the shading you used doesn't seem to have any reasoning for it. • In the System Overview, what does the system itself do? What is the sum of its parts? • In you asset inventory, you should not list ports that you don't know the purpose of them is. • Why are you using CIDR notation on your network diagram? One host will have 1 IP for this system. No need to include the subnet it is on. • The system hardening should not be a diary, but a list of steps, with justification, taken to harden each system. These should be written in a way that is repeatable in the future.

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	951
----------------------------	------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> • Good presentation! You provided strong details in describing the business and operational risks. • They had great short bullets of the presentation and I enjoyed the timeline • You started out great. Good slide layout. Good comparison of other attacks. • Risks were summarized clearly and the presentation of the risks summary was suitable for all members of the C-Suite with a very specific slide dedicated to the financial impacts. • Clearly outlined business risks and operational impact following an industrial control system compromise, with direct ties to reputation, safety, and production. • I like the examples of the risks happening elsewhere to hit home that they can and will happen. I LOVE the per day cost estimate 	<ul style="list-style-type: none"> • An area for improvement would be to provide additional detail that explicitly connects the identified risks to the proposed mitigations. Additionally, it would be helpful to include more information about the high-priority recommendations, capturing the reasons for these actions and explaining how the recommendations would reduce the risks. Furthermore, some technical jargon could be avoided considering the target audience. • More technical details backing the recommendations and what it would save the organization and what is the cost and roadmap. Some of the details around the security tools • Not only background checks, but quality of work checks for your contractors. Your strategies and high-priority

Strong Points	Areas of Improvement
<p>for any outage. Your strategies are longer term and focus on distinct categories.</p>	<p>recommendations need to be more thorough,</p> <ul style="list-style-type: none"> • Points were deducted from Presentation Time & Elements because the Team ID was not included. However the video length is approximately five minutes, there are two presenters sharing the time and they acknowledged missing team members. • Points were also deducted because not all strategies ""relate to previously identified risks"" because the hypothetical breach came from an approved vendor, doing approved work, in an area they were supposed to be in. And it is unknown if they are the attacker, or just the vector the attackers used to breach the oil rigs' systems. So access control and MFA buys no coverage (but are very important in the real world). The other recommendations, training and an intrusion detection system (IDS), meet all the other requirements for the project. • However, explaining the importance of the training and proposed IDS was an important step and would help executives make the choices to implement these recommendations. They also combine a short term and long term impact for the company • Recommendations could be more quantified (financial analysis of prevention costs versus risks) and tailored to Obsidian Rift Energy's specific environment. Vendor management could be more specific. • Your listed risks are largely just impacts, which is only one part of the equation for risk. Your strategies implicitly address similar cybersecurity incidents from happening again, but they really need to directly address the risks posed. Provide a cost estimate for your high priority recommendations, as well a justification for why they are needed right now. Why is providing requirements on contractors something you need to do right now? Is it because the current incident exposed a risk? Be more assertive in your language. Don't use phrases such as "we hope to be able to." Instead, say "we need to.

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	0	125	125

Whack a Mole		
WAM1	WAM2	WAM3
125	0	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
1475	222

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
19467.62	43.26%

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

250

<i>Green Team Survey Comments</i>
--

- Website needs a great deal of work, many aspects were incorrect or missing.
- go down the list, a lot of the site is not correct!
- Site accent color is gold/goldenrod. Nav bar has missing links and incorrect spelling. background image doesn't appear to be an oil rig, unsure what the image is. Tagline reads 'Spilling oil is good. Spilling Data is Better.' No positions listed under careers. No login button, and /login is '404 not found'. Footer info is incorrect, no street address or city, wrong company name. No logos at the top
- Color scheme is wrong, navigation is wrong, image is wrong. no login, Careers is wrong, no footer on Home page.
- Site is wrong color, tagline is wrong, no login button, footer is wrong, no careers listed, no logos in headers
- logos missing, header and footer incorrect, front page incorrect, colors incorrect, unable to login.
- This site can't be reached web.blue0073.cfc.local refused to connect.
- This site can't be reached web.blue0073.cfc.local refused to connect.