



LOYOLA UNIVERSITY CHICAGO

CYBERRAMBLERS TEAM 2

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 88 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	389	25.93%	58
Security Documentation	1062	84.96%	49
C-Suite Panel	1115	89.20%	12
Red Team	1000	40.00%	41
Blue Team	1787	89.35%	39
Green Team Surveys	1385	92.33%	35
Deductions	0		
Overall	6738	67.38%	35

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	389
----------------------	------------

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

1	Yes	10.7	Yes	17	Yes
2		10.8	Yes	18	Yes
3		10.9		19	Yes
4		11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6		11.3	Yes	22	
7	No	11.4	No	23	
8		11.5	Yes	24	
9	No	11.6	Yes	25	
10.1	Yes	11.7	No	26	
10.2	Yes	12		27.1	No
10.3	Yes	13	No	27.2	No
10.4	Yes	14		28	Yes
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	1062
-------------------------------------	-------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> Like the rankings/prioritizations of the vulnerabilities. The heat map on your known vulnerabilities was a nice touch. Detailed network diagram and logical hardening steps with good justification and explanations analysis and recommendations were thorough, they gave detailed steps into the work down and identified actions appropriately. I appreciate the color coding to identify criticality of actions. 	<ul style="list-style-type: none"> Lacks logical connections in network diagram. It would have been better to use lists in your hardening steps and map it back to the vulnerabilities found. System overview could use more simplified terms and general explanations I would recommend a second edit into written portions, while actions are well explained, there are sentences that could be tighter or omitted as it got repetitive. Pay close attention to template, some sentences were left in.

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> Extremely thorough. The report shows top-tier technical and documentation skill. 	<ul style="list-style-type: none"> Could trim redundancy. Some sections repeat similar mitigation language.

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	1115
----------------------------	-------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> I like that on the strategy you linked them to the risk and showed cost. Good work discussing the business risk Nice work embedding speaker video over slides. teamwork, presentation, clarity, good level of detail without being techy Professional visuals with comfortable pacing. The presentation was well laid out and easy to follow. Did not have to wonder what the related risks were. Professional looking slides and audio is clear 	<ul style="list-style-type: none"> Formalizing a full incident response plan in a week is a tall task. Don't talk so fast it is hard to digest the information Should state the roles and/or work performed by the other participants. Speaker volume levels are inconsistent. References could be included in a final slides for further research. Not all work could necessarily be completed by the current staff using the current software/hardware. Business Risk, Financial Bottom Line 15-30K isn't getting any attention at C-Suite, and from the other videos I was under the impression it had been weeks at 130K a day Risks should emphasize financial impact more. Strategy didn't directly address the most important identified risk - personnel safety. Dive deeper into the high-priority actions a bit more with specifics on how the tools will help. Strategy should follow risks and address each respectively. Risks section is longer than strategy and high priority recommendations. The flow of the presentation should be fluid. Addressing current events that are similar to the scenario would help the viewer understand the full scope of the plan.

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	250

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
1380	407

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)
25	23	22	23	27	27	27	27	23	26	26

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
35630.21	79.18%

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

1385

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

- Watch out extra admin user
- Address footer is supposed to be on every web page, but it's not found on the home.
- Navigation bar read 'Obsidian Energy Co.' instead of 'ObsidianRift Energy Co. ', slight name difference, no functional difficulties. Logos were absent at the header.
- No footer on the main page
- "Blue Admin and Green Admin have admin rights, which meets the requirements, but Red also has admin. There is no limitation listed for how many or which accounts have admin other than green/blue, so credit is given. Excellent work!"
- There is no footer on a home page.
- "No Footer on Home Page. Oh no, looks like you have a red user with Admin priv."
- no footer on main page, Red Admin added
- "Too many admins
- Rig page Illuminate\Database\QueryException
- Footer not on every page