



DRURY UNIVERSITY

CYBER PANTHERS

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 23 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	339	22.60%	67
Security Documentation	843	67.44%	77
C-Suite Panel	937	74.96%	63
Red Team	500	20.00%	70
Blue Team	1517	75.85%	62
Green Team Surveys	566	37.73%	79
Deductions	0		
Overall	4702	47.02%	79

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 | 339

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

1	No
2	
3	
4	Yes
5	Yes
6	
7	
8	
9	
10.1	
10.2	
10.3	
10.4	
10.5	
10.6	

10.7	
10.8	
10.9	
11.1	
11.2	
11.3	
11.4	
11.5	
11.6	
11.7	
12	No
13	
14	
15	Yes
16	Yes

17	Yes
18	Yes
19	Yes
20	No
21	
22	
23	
24	No
25	
26	
27.1	No
27.2	No
28	No
29	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 | 843

Strong Points	Areas of Improvement
<ul style="list-style-type: none">Good broad capture of fundamental mitigations and system hardening stepsGood network diagramThe system overview speaks to business interests nicely (production, strategic importance, environmental, health, and safety)System Overview concisely defines the system and ties its purpose to the industry and operations of ObsidianRift Energy. Well done!	<ul style="list-style-type: none">Not enough detail in system overview. Missing mitigation details.you had several vulnerabilities with no mitigation for those.Consider keeping formatting consistent within tables for easier reading. Be sure to include mitigations or recommendations when presenting vulnerabilities to the business.Keep consistent with the hostnames. The System Hardening section is meant to explain broad steps or categories for

Strong Points	Areas of Improvement
<ul style="list-style-type: none"> Team 23 presents a complete, accurate, and polished document, it captures both technical detail and executive-level clarity 	<ul style="list-style-type: none"> hardening and protecting the system, not simply a list of what you did for each host. Add a fully labeled, polished network diagram (with a legend and service annotations)

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"> Good coverage of operational and business risks, with a strategy that correlates Your slide presentation was very nice with limited IT jargon. Summary provided for situational awareness of C-Suite. Clear identification of risks to assets, operational and safety risks, and potential financial impacts. "Phase" alignment of strategies was an interesting touch, provided a good prioritization of actions and a flow for implementation. Able to point out financial loss and risk to the company Each idea was given its own slide. The slides were aesthetically pleasing. Addressed all talking points with a logical strategy for actions required. 	<ul style="list-style-type: none"> Does not acknowledge other team members. No mention of cost to implement high priority recommendations If you would have expanded on the risks and tie the strategies back to the risks to justify you would have had a better presentation and would have filled the time commitment. There were certain elements that were a bit unnecessary and involved some jargon that the C-Suite likely didn't need in regard to "Operational & Safety Risks". It would also be good to clarify costs associated with the high-priority network recommendations provided. Strategies to reduce risk seemed to be tactical in response to the immediate issue (short term) instead of focusing on potential long-term actions that leaders could make to help push organizational change. Be more specific on the solution The slides were simplistic should have listed tools to be used, timeline, and dollar approximations. Could have discussed specific tools and/or resources for high priority actions, provided a timeline and financial cost breakdown and referenced relatable cyber events.

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	0

Whack a Mole		
WAM1	WAM2	WAM3
125	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
1045	472

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)
17	0	17	23	17	0	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
41248.31	91.66%

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
566

Green Team Survey Comments

- The site does not load. '502 Bad Gateway' error message at the time of evaluation.
- There is an error message 'The site can't be reached'.
- Website did not load.
- "Website will not load
- Website not loading
- the website could not be reached
- site does not load
- Absolutely no access to the webpage.
- site does not load
- The website does not load. The user is met with a 'Your connection is not private' message.
- Unable to access
- "No footer on Home Page. Header drop down menu shows Admin when normal user logged in. Admin page server error 500"
- no footer on home page
- Hello Team 23, your team was only missing a footer on the main page.
- no homepage footer
- Website does not load. The user is met with a 'Your connection is not private' message.
- no footer on homepage
- Address footer is supposed to be on every web page, but it's not found on the home.
- 5:41 This site cant be reached
- 5:42 This site cant be reached
- Site is down