U.S. DEPARTMENT OF ENERGY'S CYBERFORCE COMPETITION®
DEFENDING U.S. ENERGY INFRASTRUCTURE

UNIVERSITY OF ILLINOIS CHICAGO

0X1BADB002

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 1 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	539	35.93%	24
Security Documentation	960	76.80%	66
C-Suite Panel	920	73.60%	68
Red Team	1000	40.00%	41
Blue Team	1507	75.35%	63
Green Team Surveys	1369	91.27%	51
Deductions	0		
Overall	**6295**	**62.95%**	**51**

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	539

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

1	No	10.7	Yes	17	Yes
2	Yes	10.8	Yes	18	Yes
3	No	10.9	No	19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6	No	11.3	Yes	22	
7	No	11.4	Yes	23	
8		11.5	Yes	24	
9	No	11.6	No	25	
10.1	Yes	11.7		26	
10.2	Yes	12	No	27.1	No
10.3	Yes	13		27.2	No
10.4	Yes	14		28	Yes
10.5	Yes	15	Yes	29	Yes
10.6	Yes	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	960

Strong Points	*Areas of Improvement*
• Good format, well thought out document, suitable for senior leadership • The team identified a realistic range of system weaknesses and offered practical mitigation strategies that show solid technical understanding. The document is well organized and written clearly, making it easy to follow. The overall layout demonstrates a thoughtful approach to both content and presentation. • System overview was concise, short and sweet for high-level decision makers without a lot of jargon. Mitigations for listed	• System description was far too short and simple. Missing 2 of 6 VMs. Router IP is outside of subnet. • "The vulnerability section would benefit from separating findings and mitigations into two distinct areas and adding severity levels or CVE identifiers for each issue. • It would also be helpful to align the listed ports and services with the asset inventory for accuracy and consistency. • Finally, the addition of a short business context section would help leadership

Strong Points	Areas of Improvement
vulnerabilities were sound, technically competent, and reasonable. Network diagram made logical sense. • Overall the security documentation was thorough and covered the requirements. • Network diagram included all components and was appropriate for the audience.	understand the operational impact of vulnerabilities." • AD/HMI were missing from the asset inventory. It'd be good to give a best-practice justification for the steps taken in plain-language for leadership for each aspect you discuss. • A few areas that could have been stronger include greater detail about the systems and their purpose in the System Overview. While an impressive 34 vulnerabilities were listed, two hosts were not mentioned. • Asset inventory was incomplete or not comprehensive.

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	920

Strong Points	Areas of Improvement
• Michael did an excellent job speaking. Excellent slides and graphics. • Good focus on safety. Strategy is confined to cybersecurity actions and is not clearly connected to previously identified risks. Strategy does include immediate and long term considerations. Focused on high priority recommendations and clearly connected them to previously identified risks with minimal costs. • the presentation layout was good. • Complete and Clear Strategy: The team provided a complete strategy containing three long-term action items designed to reduce risk: 1) Containment/quarantining of compromised networks, 2) Installation of logging and monitoring software, and 3) Hardening of services/software. This strategy clearly addressed the identified risks (halting hacker influence and preventing future breaches). • Justified, Low-Cost Recommendations: The team provided 3–4 high-priority actions with complete and consistent reasoning. Crucially, the recommendations adhered to the constraint that current funding is extremely limited, proposing actions that	• No financial impact was provided nor was there a cost given to execute the 3 high priority recommendations. While you considered social media hacking of the contractor, is it possible that the contractor was a malicious actor? Could you also prohibit any removable IT devices until scanned by the cybersecurity team? • Risks to financial bottom line should be made evident. Strategy should extend beyond cybersecurity actions and should be connected to previously identified risks. • less jargon and acronyms • Explicitly Link Risks to Financial Bottom Line (Category B): While the team clearly identified severe operational risks (40-second site-wide blackout, machinery interruptions, and the dangerous gas overpressure incident) and linked these to safety (""real human lives"") and production (""hosting our production lines""), the presentation only achieved a Proficient score in this category. To achieve an Exemplary score, the team needed to clearly identify how these risks affect the company's bottom line (finances). For instance, quantifying the financial impact of

Strong Points	Areas of Improvement
require at most a minimal level of additional funding by focusing on actions that only cost ""a little bit of time"" (e.g., better contractor screening) or ""goes a long way"" (e.g., raising social engineering awareness). This approach demonstrates a strong understanding of the audience (C-Suite) and the task constraints. • The video didn't interfere with the slides themselves, all topics were well covered, and the slides looked good. • Covered and outlined business risks and operational impact.	halted production or the potential cost of reputational damage was required. • Future presentations should ensure speaking time and active roles are shared among more than two team members and also try to use better camera quality for better viewing of the presenters. • You should have taken the time to introduce your team, mentioning their names and contributions, the slides had a lot of information on them, more slides would have made the presentation easier to digest. • Recommendations could be more quantified (financial analysis of prevention costs versus risks) and tailored to Obsidian Rift Energy's specific environment.

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	125	0	125	0	125

Whack a Mole		
WAM1	WAM2	WAM3
125	250	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
1405	102

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	27	27	16	25	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
8979.84	19.96%

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
1369

Green Team Survey Comments
• Few things recommend fixing as I feel they are coding issues vs attack issues - your footer should probably appear on the home page even and when you minimize the screen and get the collapse menu vs the menu across top the Admin option appears when logged in as normal user - good news it does validate user not admin though and says unauthorized access, but you probably want to fix that collapse menu so it doesn't show Admin either like you have on the normal full screen.
• No footer in the main page.
• Great job Team 1, and good luck defending your oil rig!
• Could not scroll on the Main Home Page to verify the footer text was present. Good luck!
• footer text not on home-screen,
• Homepage needs a footer
• footer text missing from home page
• The footer is not on every page. It is missing on the home page, login page, and signup page.
• footer not showing on main page
• Footer not on every page
• Footer not on every page
• Site is down