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

INDIANA INSTITUTE OF TECHNOLOGY

INDIANA TECH CYBER WARRIORS

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 52 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	354	23.60%	64
Security Documentation	1036	82.88%	54
C-Suite Panel	939	75.12%	62
Red Team	875	35.00%	44
Blue Team	1817	90.85%	36
Green Team Surveys	1330	88.67%	48
Deductions	0		
Overall	**6351**	**63.51%**	**48**

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	354

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		10.9	Yes	19	Yes
4		11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6	No	11.3	Yes	22	
7	No	11.4	Yes	23	
8	No	11.5	Yes	24	No
9		11.6	Yes	25	
10.1	Yes	11.7	Yes	26	
10.2	Yes	12		27.1	
10.3	Yes	13		27.2	No
10.4	Yes	14		28	No
10.5	Yes	15	Yes	29	
10.6	Yes	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	1036

Strong Points	*Areas of Improvement*
• This report is technically strong, with thorough vulnerability coverage and clear explanations. • The mitigations are realistic, and the structure of the document is professional and easy to navigate. • The team demonstrates solid command of both Windows and Linux system security concepts. • Vulnerability mitigations were appropriate for the audience, and your list was very thorough. • Future Recommendations	• There are a few mismatched mitigation notes, such as SSH configuration findings linked to SMB corrective actions; these should be reviewed and corrected. • Each vulnerability should include a severity rating and confirm that the mitigation applies to the same host. • The network diagram should be labeled with system names and a simple legend for clarity. • Finally, summarizing the top few risks in a short executive summary would make the

Strong Points	Areas of Improvement
	document more accessible for non-technical readers. • "Standard practice is to use different icons for different types of assets in the network diagram, with a key. • Your hardening steps reads like a diary. Why did you take each step? What is the justification? What is the benefit? • I would recommend more statistics for the recommendation next steps

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	939

Strong Points	Areas of Improvement
• great work handling with 2 members • I like that you added the colonial pipeline incident for comparison. • Information presented was valuable, and related to the topic. Team dressed professionally • Included communication and investment strategies as risk-reduction measures. • Good coverage of high priority recommendations • Good work on citations.	• use $$$ for business concerns • Avoid jargon for C-Suite. Holding papers in front of you was distracting. More thought was needed for the risks and strategies. • The presentation could've been improved. The risks and strategy needs to be more related and following the recommendation. A clear time line could've been a good way of presenting a strategy. • Never actually addressed what the incident was. • Holding the papers seemed unnecessary and the sound the paper made was slightly distracting. • Identified roles of staff members • Operation Concerns should be phrased as Risks. Should be quantified financially. • Speaker volume is low. Consider using microphones or standing closer to the camera, or using Zoom to recored. • More details needed on strategies to reduce risk, high priority recommendations : costs, staffing, timelines, software and hardware needed, training for staff, etc. • Real World Impact should have a different title this is a presentation to the C-Suite regarding an on-going incident, they are living the real world impact. Could be phrased as future risks or future potential impacts.

Strong Points	*Areas of Improvement*
	• Could also end asking for the viewer to reach out if they have further questions.

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	125	0	0	0	0

Whack a Mole		
WAM1	WAM2	WAM3
250	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
1475	342

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
29897.50	66.44%

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
1330

Green Team Survey Comments
• there's no management button. • Blue and green admins missing • The homepage does not have a footer. Under the Admin User Management, there was only one user listed. • 'blue@obsidianrift.oil' and 'green-admin@obsidianrift.oil' not included in user management page. no footer on home page. • no footer on main page. blue admin and green admin not showing on user page • No admin accounts listed under User Management when logged in as green-admin. Other than that, it was excellent. • No footer, no admin users. • Good job • Good job • Extra admin account • site cannot be reached