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

PURDUE UNIVERSITY NORTHWEST

ROAR CYBER CLUB

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 74 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	268	17.87%	80
Security Documentation	1218	97.44%	5
C-Suite Panel	975	78.00%	53
Red Team	750	30.00%	53
Blue Team	1445	72.25%	75
Green Team Surveys	818	54.53%	70
Deductions	0		
Overall	**5474**	**54.74%**	**70**

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	268

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

1	No	10.7		17	Yes
2		10.8		18	Yes
3		10.9		19	Yes
4	Yes	11.1		20	Yes
5		11.2		21	
6		11.3		22	
7	No	11.4		23	
8	No	11.5		24	No
9	No	11.6		25	
10.1		11.7		26	
10.2		12	No	27.1	No
10.3		13		27.2	
10.4		14		28	No
10.5		15	Yes	29	No
10.6		16	No	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	1218

Strong Points	*Areas of Improvement*
• The team provided a plain-language system overview tailored for senior leadership, a complete asset inventory listing all six VMs and their details, and a comprehensive network diagram that included all assets, logical connections, and a legend. Furthermore, the vulnerability section exceeded requirements with many documented items presented professionally, and the hardening plan was robust, detailing multiple defensible steps like segmentation and patching that were justified by risk reduction.	• six key actions to improve the report. First, enhance professionalism by fixing all typos and replacing vague "Will/Need to" language with a clear "Resolved vs. Open" status. Second, create an executive summary table that totals vulnerabilities by host and by status (mitigated vs. open). Third, detail the network segmentation using a "zones and conduits" model aligned with NIST SP 800-82, specifying allow-list rules. Fourth, document the monitoring and response plan, listing log sources, alert triggers, and uptime targets. Fifth, explicitly

Strong Points	*Areas of Improvement*
• The system hardening was easy to follow and thorough. • The report was technically sound and well put together. • Covered great amount of details with clarity and looking good to present. Overall great effort by the team. • this document was well formatted, while it targets senior audience, a non technical person can follow analysis and recommendations well.	state the "assume-breach" constraints and formally record any unfixable issues as "accepted risk" with compensating controls. Finally, improve the patching process by documenting backup/restore validation and change control procedures. • The system overview still used technical language in some spots that could have been too complex for a c-suite. • The report could use editing, fix typos, remove some jargon. • There can be more details added to system hardening section. • charts could be improved a bit to better identify information

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	975

Strong Points	*Areas of Improvement*
• The presentation was clean and professional looking. • Good work quantifying the risks • slick, simple, to the point, and high level. • Very good job at quantifying downtime. High priority recommendations are well thought out, and you tie them back to the risks. • Strategy ties into risks identified and high priority recommendations. • Clear and professional presentation and the video of the team presenting it.	• I would have liked more details on your strategies and recommendations. • State the work roles and work completed by other team members • Images seem Ai generated but are not cited as AI. • Mitigation, include specifics such as costs, staffing, software, hardware requirements, and training requirements. • Some jargon, recommend phrasing to ensure C-Suite non tech experts can comprehend. • Recommend including references • training staff on password management doesn't align with the challenge technically vs being broader good practice. • Your listed risks are largely just impacts, which is only one part of the equation for risk. Don't claim that your strategies will prevent risk, only that it will reduce risk. I like your strategies, but how do they reduce the risks you outline? How do they reduce the impact of safety? They implicitly reduce risk by reducing the likelihood of another incident occurring, which in turn reduces the safety impact. Don't make the

Strong Points	*Areas of Improvement*
	C-Suite make all the connections on their own. Be direct about the connection. • Strategy could have been corelated with risks identified more tightly. • Tables or charts added for emphasis to the key recommendations.

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
125	0	0	125	125	0	0

Whack a Mole		
WAM1	WAM2	WAM3
125	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
1345	100

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	25	27	24	25	17	27	16	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
8741.30	19.43%

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
818

Green Team Survey Comments
• The photo was on the page, but not fullscreen
• Nothing on login page
• Was not able to sign in, clicking 'login' did not bring up a login page
• the tag line is Spilling Oil is Bad. Spilling Data is Worse.
• your tagline is wrong, we are unable to log in, and your logos are not in between the navigation buttons. Also, while your rig status page does give operational/not operational status, the site is very off.
• logo looks ok.
• This site has a different style / layout than what is on the rubric. Login functionality is not working.
• Couldn't log in.
• how to apply for the jobs listed in careers? login field doesn't show
• Login button does not work. Tagline is wrong
• login link does not work + tagline is wrong
• your tagline is incorrect, we are unable to log in, while your rig status does give adequate information its site is off, and your logos are not between the navigation buttons.
• This site can't be reached
• "The pages should be within the top bar Login doesn't work"
• web.blue0074.cfc.local refused to connect.
• web.blue0074.cfc.local took too long to respond.