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

NEW MEXICO TECH

PUSHPOP

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 68 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	404	26.93%	54
Security Documentation	921	73.68%	70
C-Suite Panel	745	59.60%	90
Red Team	500	20.00%	70
Blue Team	1470	73.50%	74
Green Team Surveys	1295	86.33%	77
Deductions	150		
Overall	**5185**	**51.85%**	**77**

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	404

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

1	No	10.7	Yes	17	Yes
2	No	10.8	Yes	18	Yes
3		10.9		19	Yes
4		11.1	Yes	20	Yes
5	Yes	11.2	No	21	
6		11.3	Yes	22	
7	No	11.4	Yes	23	
8		11.5	Yes	24	No
9	No	11.6		25	No
10.1	Yes	11.7		26	
10.2	Yes	12		27.1	Yes
10.3	Yes	13		27.2	Yes
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	921

Strong Points	*Areas of Improvement*
• Overall the writing portions were well done and well written. • The system overview description including both the technical purpose and the business standpoint was a great idea. The host name being listed on each device in the network diagram was good! Not all groups chose to this. Adding this helps less technical people follow the diagram. • Great job on the asset inventory and getting most of the ports in. • Hardening Recommendations	• The assets table could be better organized to allow the senior leadership to follow this better. The diagram doesn't convey the full information with logical connections. Only a limited number of vulnerabilities were found and mitigated. • Make sure to spell out all acronyms before being used (e.g., IT, SSH, etc.) PLC missing port 502.DB missing ports 80 and 3306. Service SMB missing. HMI missing ports 8088 and 3306. Network diagram should show all hosts touching the router.

Strong Points	*Areas of Improvement*
• The report was clear, fairly concise, and the content was solid.	• Sections had great starts to them but just needed to be expanded out more. The system hardening could have used some more justification beyond saying it will make the system more secure. • Network Diagram could have been improved • The formatting could have been clearer to delineate elements and highlight important parts.

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	745

Strong Points	*Areas of Improvement*
• Good inclusion of a timeline and suggested incident response steps, very appropriate for C suite. • You had good information. • The presentation was well given. • This presentation provides a thorough risk assessment, actionable recommendations, and a clear timeline, using open-source tools and practical strategies that are highly relevant for C-suite leadership. • Well presented the strategy and recommendations.	• Video is blocking slide text. Did not mention contributions of team members. Strategy is focused on the incident and only loosely connects to business and operational risks. • The presenter video blocks text on slides. Too much IT jargon for C-Suite. Presenters were reading from a script, making it sound robotic. The splicing of the videos was very distracting. You could also expand on the risks and strategies. really show the value and the cost. • Some slides had lots of wording with several of the slides having the info blocked by the video boxes. The business risks needed to be tied back to the financial bottom line. • The presentation could be improved by providing more specific details on how forensic imaging and firmware verification will be conducted and by clarifying roles during each phase of the response. • Risks could've been explained further and with more details, everything start from the risks. The videos were covering some of the text on the slides.

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	250	0	125	0	0	125

Whack a Mole		
WAM1	WAM2	WAM3
0	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
1470	0

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	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
0.00	0.00%

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
1295

Green Team Survey Comments
• Footer is visible on every page except the homepage • no manage button after login. • Address footer is supposed to be on every web page, but it's not found on the home. • company name misspelled, green user not on user management screen, • footer not available on main page, company name misspelled, green user not on user management • No footer on homepage, Login, or Sign Up. Nice work otherwise! • Don't forget the Rift in ObsidianRift! You also do not have a footer on the front page. • Good job but recommend like the other pages to put the footer on home page • Rock-solid work! Even Obsidian Rift's rigs approved Unfortunately, you're missing the footer on the home, login, and signup pages. • Footer missing from main page • Good job! You are missing the green user within the User Management section and your rig is currently 'Not Operational'. • website is down • web.blue0068.cfc.local refused to connect.