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

UNIVERSITY OF MARYLAND, BALTIMORE COUNTY

UMBC CYBERDAWGS

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 90 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	510	34.00%	32
Security Documentation	1187	94.96%	14
C-Suite Panel	1027	82.16%	41
Red Team	1250	50.00%	27
Blue Team	1904	95.20%	19
Green Team Surveys	1301	86.73%	30
Deductions	0		
Overall	**7054**	**70.54%**	**30**

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	510

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

1	Yes	10.7	Yes	17	Yes
2		10.8	No	18	Yes
3		10.9		19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6		11.3	Yes	22	
7		11.4	No	23	
8		11.5		24	
9	No	11.6		25	
10.1	No	11.7		26	
10.2	Yes	12		27.1	Yes
10.3	No	13		27.2	Yes
10.4	Yes	14		28	Yes
10.5	Yes	15	Yes	29	No
10.6	No	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	1187

Strong Points	*Areas of Improvement*
• Excellent asset inventory; colors are a nice touch. Best overall submission by any of my 12 teams that I graded. • Love the color coding! Overall excellent submission. • Covered great amount of details with clarity and looking good to present. Overall great effort by the team. • Color coding throughout document was a nice touch. The system hardening is really well formatted and helps the c-suite identify key takeaways from the headers and overviews provided. Nice job!	• System overview - comments about Asset Inventory shouldn't be there. Vulnerability listing - use CVE descriptions vice numbers for senior staff use • Would have been great to see the color coding in the network diagram, too. Also network diagram needs to show logical connection between services. • Too many colors are not required and specific readable formatting can help. • System overview should include mention of breach in system. Web server OS should be OpenSUSE Leap. I would include the blue

• The color coding on each asset was a thoughtful touch that added clarity and made the documentation easy to understand at a glance. Your system hardening section was also very strong and showed solid technical reasoning.	icons on the servers in the legend to help the audience understand what each of those mean. If they do not have a meaning, then remove them. In known vulnerabilities, the CVEs should be described so the c-suite can understand what the information means. There is no introduction to the vulnerabilities section that would indicate what a CVE is or where they can look them up. Typo in PII section. • Including brief mentions of the tools you relied on for hardening would strengthen the context behind your decisions. The work itself was strong and adding that information will help highlight the effort and reasoning you brought to the task.

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	1027

Strong Points	*Areas of Improvement*
• The risks and potential impact section was particularly effective, especially in using financial data. The slides were well organized and effective overall, especially in using short bullet points over sentences. Also, good job citing references. • A clear response plan is key. • Nice job! Easy to follow. • You used a slide layout that made it so the video didn't cover up your slides. The Risk and Potential Impact slide graphic was well done. Spoke to the slide instead of just reading off of them. • The strategy to reduce risks and high priority actions are clear and concise. • Cost aside, the high priority recommendations were strong.	• Both the risk reduction strategy and high priority items would benefit from greater specificity in implementation. While I know it wasn't supposed to be overly technical and jargon-y (and this did a good job avoiding that issue), it would benefit from mentioning, for instance, which particular tools you would use to implement some of those recommendations, even while staying at a high level. This would also help address the question of how much each action items would cost to implement, which would have improved the presentation as well. • Wearing a hat during a C-Suite presentation is not professional. Audio volume is low. There are more risks to consider. • The 3rd speaker could have slowed down. You should have suggested tools that you would be using. • Be clear on what the exact risks are for not having adequate cyber security and how that would overall the company. • The mitigation strategy hardly mentioned the aforementioned risks. Do we know the cost of the high priority 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
0	250	125	125	0	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
1475	429

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
37510.27	83.36%

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
1301

Green Team Survey Comments
• I recommend you adjust your home page, you do have the footer on the other pages so I am going to mark this true as I don't think this is a defend issue but possibly a issue with your html, others reviewing site might think differently though so I recommend you fix. Address not on home-screen"
• No footer on the main homepage.
• Excellent work!
• footer not on main page
• "no footer on main page, the learn more button is blue
• Footer missing main page.
• Footer not on every page
• footer missing on main page
• 5:46 This site can’t be reached
• web.blue0090.cfc.local refused to connect.