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

BALDWIN WALLACE UNIVERSITY

BW CYBERSEC

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 12 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	772	51.47%	7
Security Documentation	1160	92.80%	19
C-Suite Panel	856	68.48%	84
Red Team	1250	50.00%	27
Blue Team	1926	96.30%	13
Green Team Surveys	1388	92.53%	17
Deductions	0		
Overall	**7352**	**73.52%**	**17**

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	772

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	Yes	19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6	Yes	11.3	Yes	22	Yes
7	No	11.4	Yes	23	
8	No	11.5	Yes	24	
9	No	11.6	Yes	25	Yes
10.1	Yes	11.7	Yes	26	
10.2	Yes	12	No	27.1	Yes
10.3	Yes	13	No	27.2	Yes
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	1160

Strong Points	*Areas of Improvement*
• I liked the formal recognition of the need for recovery. • Excellent use of the NIST “Identify, Protect, Detect, Respond, Recover” model. • Great use of free tools and explanation as to why each tool was utilized. Implementing NIST's framework and identifying the outline of the framework before speaking to it is critical in giving senior leadership enough information to understand why you chose what you did and how it is to be implemented. • Easily understood network diagram	• In documentation, host names are generally intended to be human readable (rather than just listings of EC2 IDs). • Could add a bit more technical evidence • Need to define CVSS in system overview and charts should have context with them. OS for Webserver should've been OpenSuse Leap, not SLES. Public DB host should have port (service) 139/445 (SMB). Hosts in asset inventory should be spelled out for senior leadership to understand what an AD/DNS is, and to restate what PLC and

Strong Points	Areas of Improvement
	HMI are. Any acronym should be spelled out before being used (NIST, SOC, etc.). • Asset inventory table may be difficult to read for senior leadership

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	856

Strong Points	Areas of Improvement
• The student demonstrated good preparation but relied heavily on reading throughout the presentation. While using notes can be helpful, it's more engaging when the speaker connects with the audience directly rather than reading word for word. Practicing more eye contact and natural delivery would strengthen the overall impact. • Strong point for this entry was the easy-to-understand method that was used to present content. Extraneous details and technical jargon did not drag down the pace. Strategies to reduce risk were sound recommendations that covered policy and technical controls. High priority recommendations were reasonable with a low cost. • Recommendation to better vet third-party risk • Strategies are sound, but they don't specify how they reduce risks (because there weren't really risks specified). • Team explained incident well and provided good recommendations and follow up actions. I like the focus on the bottom line driving their point on why their solutions are appropriate. • Good high priority recommendations	• The students could have strengthened their proposal by suggesting ways to leverage modern technology, such as AI platforms, to automatically streamline the process of vetting contractors before hiring. good job overall • Although the content was easy to understand, some slides felt a bit text-heavy. The prioritization and presentation of risks were occasionally unclear (for example, using "Compensation" as a header may have distracted from the more critical issue of worker health risks). It might be more effective to address the operational impact of the outage first, then discuss the financial implications such as compensation claims. Including a rough cost estimate based on lost oil output would help quantify the impact. It could also be useful to briefly note the confidentiality-related impacts as bullet points for completeness. • Unclear how backup devices recommendation would have affected the event. The recommendations to strengthen security and enhance monitoring lacked detail and felt like they could have been combined into one recommendation. No details about which third parties should be notified or coordinated with. • "Risks are a product of likelihood and impact. What is the likelihood and impact of different cybersecurity threats to the organization? • What is the cost of the high priority recommendations? How do they reduce the risks you specified?"

Strong Points	*Areas of Improvement*
	• Some of the content seems disjointed, the solutions and risk • are explained as if separate from each other. No clear connection from one to the other. Some of the analysis can be deepened. • You need to tie everything back to the bottom line. All risks, which lead to your mitigations strategies and high priority actions.

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	250	0	0	125	0	0

Whack a Mole		
WAM1	WAM2	WAM3
250	125	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
1485	441

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	27	27	27	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
38564.37	85.70%

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
1388

Green Team Survey Comments
• Positions of interest on the careers page cannot be applied for.
• incomplete career page
• You have the positions listed and have a spot in the form but no way to select it, please update so the next person gives you credit.
• Excellent work!
• No footers on the login page.
• Rock-solid work! Even Obsidian Rifts rigs approve" though you're missing footers on the login and signup pages, and the career page needs position descriptions.
• red filter not present over oil drill picture
• Good work! All intended areas are still accounted for within the website and no issues locating anything per the requirements. One thing is the accent color is not on the image itself when the website boots up, but otherwise everything is good to go!