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

AUBURN UNIVERSITY

AUBURN WAR D— TIGER EAGLES

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 22 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	514	34.27%	30
Security Documentation	1178	94.24%	16
C-Suite Panel	1179	94.32%	5
Red Team	1500	60.00%	14
Blue Team	1838	91.90%	32
Green Team Surveys	1304	86.93%	8
Deductions	0		
Overall	**7513**	**75.13%**	**8**

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	514

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

1	Yes	10.7	Yes	17	Yes
2	Yes	10.8	Yes	18	Yes
3	No	10.9	Yes	19	Yes
4		11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6		11.3	Yes	22	No
7	No	11.4	Yes	23	
8		11.5	Yes	24	
9	No	11.6	Yes	25	Yes
10.1	Yes	11.7		26	
10.2	Yes	12	No	27.1	No
10.3	Yes	13		27.2	No
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	1178

Strong Points	*Areas of Improvement*
• Good job extracting compromised files for analysis and not simply deleting/replacing. • The vulnerabilities table was very thorough • Covered great amount of details with clarity and looking good to present. Overall great effort by the team specially in the vulnerability listing and system hardening section. • The system hardening was an extensive list of changes made to each system. The inclusion of tools used for each device being listed after each device was very helpful and the overall formatting of this section made it	• PLC IP address incorrect in asset inventory does not match diagram, considered a major error, see rubric footnote. Stronger justifications needed for steps taken in system hardening, many steps had no justification provided. • system and purpose are well defined but not targeted to senior leadership. The diagram gave several assets that were not included in the assets list. System hardening reiterated some specifics from the vulnerabilities table, but should be more of a broad overview of what was done. It

Strong Points	Areas of Improvement
easier for the audience to follow. Further description of certain tools and functions would push this paper to the next level.	was also a bit tedious to go through, and need to be simplified for senior leadership. • Network diagram can use symbols for n/w diagram instead of pics and there can be more clear details about ports and connections. • Make sure to spell out all acronyms before being used. When introducing any topic you should describe what it is and what it does (Modbus protocol in the system overview) so those who do not know prior to reading will be able to understand what you are saying (assume C-suite has no technical knowledge). Hosts in asset inventory should be spelled out for senior leadership to understand what an AD/DNS is, and to restate what PLC and HMI are.

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	1179

Strong Points	Areas of Improvement
• Great job quantifying costs for risk categories such as EPA fines, equipment damage/replacement, and revenue loss. Also, speakers were well-rehearsed and slides well-designed (e.g., the use of tables was effective for risks and high priority actions). • Good inclusion on the estimated costs to implement risk reduction strategies. Very convincing explanation of business and operational risks • Your proposals strongly related to the identified risks and were layed out very clearly in the presentation. Great job displaying cost assessments regarding operational impact and in your high priority recommendations. • This had a great identification of risks in an easy-to-read table. Priority for these risks aligned with executive concerns and kept financial aspects at the forefront. Strategies to reduce risk were sound and included both technical and policy changes that were reasonable.	• While you did a great job attempting to use low cost high priority actions, some of them would have cost money. For instance, security training for staff costs money for the material, instructors, and to cover staff time while being trained. • Slides have too much text to consume. Strategy is directly related to the incident more than the operational/business risks. • Risk reduction strategies could have tied into identified risks better - for example, I did not see the risk of Personnel Safety clearly tied back in your risk reduction strategies. • Unfortunately, the presentation went over the time limit. The security incident timeline was a solid and informative start, but it occupied a large portion of the presentation. It also included a lot of “and then this happened” detail and delved into some overly detailed elements that are not directly helpful to the C-Suite. That time might have been better spent focusing on

Strong Points	*Areas of Improvement*
• Financial Quantification of Risk: The team provided a clear summary of business and operational risks and successfully quantified these risks, directly linking the security failure to the company's bottom line. The presentation identified specific financial impacts, including potential EPA fines (e.g., $50,000 to 2M to 150,000 per day in production interruption). This detailed quantification ensured the risks were clearly identified and suitable for all C-Suite members. • Minimal Funding Requirement: The recommended high priority actions, which included strengthening IT/OT boundaries and deploying continuous ICS monitoring, were explicitly designed to leverage open-source tooling and existing hardware. This demonstrated compliance with the critical requirement that actions require ""at most a minimal level of additional funding"", emphasizing a strong return on investment (ROI) that leadership seeks. • Structural and Professional Excellence: The team met all required elements for the video, including having three active participants, providing clear acknowledgment of contributions from all six team members (Hemant, Will, Luke, Enoch, James, Matthew), and maintaining a professional appearance with a ""well dressed"" team and good slides. • Thorough understanding of regulatory impacts and financial risks, and a stepwise methodology for risk management along with good financial data. • High-priority actions were excellent, IT/OT segmentation absolutely takes the #1 spot!	the key risks, impacts, strategies, and recommendations. • Explicit ROI for Every Recommendation: While the team successfully established the overall ""low-cost, high-impact strategy"", further explicitly detailing the return on investment for each of the four high priority actions would enhance the persuasion. For instance, directly linking the proposed workforce readiness training or vendor access management improvements to the immediate reduction of a specific, high-cost risk (like the potential $500,000 daily fine) would solidify the justification even further. • Integrating Investigation Detail: The strategy included ""Restoration and Investigation"" with special scrutiny toward contractor access. An improvement would be to more explicitly integrate the long-term actions (like strengthening vendor access controls) with the initial incident timeline, reinforcing how the recommended solution directly prevents the specific vector of attack identified by the response team. • Clarity of Policy/Staff Changes: The task requested discussion of recommended staff communication, training, and policy changes. While the team addressed training and workforce readiness, providing slightly more detail on the specific policy updates (e.g., the policy changes needed for vendor access management or enforcing strict least privileged access controls) could further strengthen the ""Strategy to Reduce Risks"" component. • Vendor management could be more specific. • The incident timeline and costs sections took a bit more of your 5-minutes of C-suite time than I would have expected, but the information was overall very well presented

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	125	250	125	0	0	125

Whack a Mole		
WAM1	WAM2	WAM3
250	250	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
1435	403

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	24	23	26

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
35262.80	78.36%

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
1304

Green Team Survey Comments
• No issues. • Great job, good luck! • logos wrong order. • "On the career page, the options are listed so I didn't deduct the point but the positions didn't have the details about each position. Great job!" • Excellent Job Team 22! I really like your career page set up! Good luck on defending your oil rig! • red user added, logos flipped around • 5:40 504 Gateway Time-out • "This site cant be reachedweb.blue0022.cfc.local refused to connect. Try: Checking the connection Checking the proxy and the firewall ERR_CONNECTION_REFUSED" • Site is down