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

HIGHLINE COLLEGE

THUNDERBIRDS

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 34 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	281	18.73%	78
Security Documentation	1088	87.04%	42
C-Suite Panel	1076	86.08%	28
Red Team	375	15.00%	77
Blue Team	1365	68.25%	81
Green Team Surveys	124	8.27%	81
Deductions	0		
Overall	**4309**	**43.09%**	**81**

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	281

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

1	Yes
2	No
3	No
4	No
5	No
6	No
7	No
8	No
9	No
10.1	No
10.2	Yes
10.3	Yes
10.4	Yes
10.5	Yes
10.6	Yes

10.7	No
10.8	No
10.9	No
11.1	Yes
11.2	Yes
11.3	Yes
11.4	No
11.5	No
11.6	No
11.7	No
12	No
13	No
14	No
15	Yes
16	Yes

17	Yes
18	Yes
19	Yes
20	Yes
21	No
22	No
23	No
24	No
25	No
26	No
27.1	No
27.2	No
28	No
29	No
30	No

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	1088

Strong Points	*Areas of Improvement*
• system well defined and in plain language for senior leadership. • Very strong and complete technical coverage. Good network diagram. • The network diagram looked great. • Overall the entire entry for this team seems quite strong, the asset list and description of ports, protocols, the network diagram including the legend, logical connections and mapping were all great. Next up the vulnerabilities captured and mitigations, hardening suggestions were all appropriate and demonstrated the team's investigative	• Asset inventory is quite long. • Some spelling and grammar problems. Some phrases are vague or informal. • You should call out acronyms the first time you use the full phrase. • This is a great team effort and I'm really struggling to come up with any suggested improvements for the report. Great job!

Strong Points	*Areas of Improvement*
skills. The report was well organized and professional.	

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	1076

Strong Points	*Areas of Improvement*
• Your use of visuals in the presentation was very good. They helped me clearly understand the risks you identified and your recommendations. • The risks were clear in pointing out how the bottom line would be affected with each risk. • Well presented and explained • Very good to include things like loss of reputation as a risk - sometimes loss of reputation or trust is more impactful than the immediate dollar value. • Overall a great video, you all did a great work getting all team members to participate in a way that's applicable to the C-suite • Directly addressed aforementioned risks.	• This is very nit-picky, but you may consider focusing more in-depth on how a few specific open-source tools can directly benefit you in terms of the scenario, rather than briefly glossing over 6 of them. • Slides have a lot of words, the graphs were hard to read, and the video visuals were distracting since they were all different shapes and moved around the page with each slide instead of being consistent. Risks were addressed in isolation and not as a whole. Strategy and recommendations were not tied back to the risks and business concerns. • The risk were presented in isolation, not short or long term identified for the strategy. • Open source solutions options was more in the weeds than the CISO needs. Strategy and mitigations do not have clear ties back to risks. • I would have liked to see more about network segmentation or firewalls to better isolate the OT risks from IT infrastructure • You could have more thoroughly addressed mitigating risks to physical safety.

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	0	0	0	125	0	0

Whack a Mole		
WAM1	WAM2	WAM3
0	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
1365	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)
18	17	24	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
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
124

Green Team Survey Comments
• site is not loading

Green Team Survey Comments
• This site is compromised; color scheme, text do not match the rubric, no Admin, no footer.
• "The color was yellowish. No login menu. No image on the homepage. No tagline is listed. No career options listed. Footer address is incorrect; The rig-status page came back with the error below; 'Internal Server Error SQLSTATE[HY000] [2002] Connection refused (Connection: mysql_historian, SQL: select * from `production`)' No logos are listed.
• Wrong color, login is unavailable, all career listings missing, no oil rig image or tagline, no footer on homepage, cannot access Rig Status page, and logos missing from navigation bar.
• Most website functions are dead.
• 404 not found
• Wrong color, no login button, unable to load rig status page, no careers listed, no logos in header, no image on main page.
• Incorrect footer info, cannot login, careers missing, etc.
• Rig status error
• can't log in, missing image, tagline, footer info, wrong color, etc.
• Site is down
• 5:51 This site cant be reached
• Site is down