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

EMBRY-RIDDLE AERONAUTICAL UNIVERSITY PRESCOTT

XORING 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 98 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	525	35.00%	28
Security Documentation	812	64.96%	83
C-Suite Panel	972	77.76%	55
Red Team	1000	40.00%	41
Blue Team	1946	97.30%	10
Green Team Surveys	1383	92.20%	38
Deductions	0		
Overall	6638	66.38%	38

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	525

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

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

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

17	Yes
18	Yes
19	Yes
20	Yes
21	
22	
23	
24	
25	
26	
27.1	Yes
27.2	Yes
28	Yes
29	
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	812

Strong Points	*Areas of Improvement*
• Assets table was well organized • Tables were well organized. • Recognized value of communication and change management as a hardening step • Well done on the asset inventory and on the network diagram.	• System overview gave limited information about the system. Some vulnerabilities missing appropriate mitigation steps. System hardening did not give justification for why mitigations steps were or were not taken. • System overview gave limited information about the system and did not well define the system. The diagram gave an overview of the system but lacked in system connections. Some vulnerabilities missing appropriate mitigation steps. System hardening did not give justification for why

Strong Points	*Areas of Improvement*
	mitigations steps were or were not taken and gave very little information overall for the hardening of the system. • Most hardening steps were remediation. Listing CVE numbers with no context is not a suitable level of detail for the audience. • The system hardening could use elaboration on both the overall steps you want to take and the strong justification for those steps.

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	972

Strong Points	*Areas of Improvement*
• Good visual aids. • Strategy is acceptable and have potential • Appropriate level of detail • The presentation looked professional • Like able to identify risk and develop solution • Very c-suite language, "Risk Posture" was excellent; as well as solution alignment to the cause of the breach, and mitigating this specifically in the future; vs generic cyber security uplift.	• No video of participants. More details on specific risks and strategies. You are creating an IDS what about an IPS. Justify the costs a little more. • The risk could be presented better not clearly explained and identified. The strategy and recommendation, therefore, are difficult to be tracked to help solve the risks. Not able to see the dress of the presenters, no camera shown. • Risks were unclear • Minimal summary of risks. You could have spent more time there. • quantify the cost of the loss in production vs just stating there was one. If they've got a fleet of rigs im guessing they all have different outputs, so quote the impact financially.

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	0	125	0	125	0	125

Whack a Mole		
WAM1	WAM2	WAM3
125	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
1450	496

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	25	24	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
43403.16	96.45%

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
1383

Green Team Survey Comments
• logos in wrong order

Green Team Survey Comments
• The careers were there but no links. There was an admin button when logging into this site. • Great job! • All elements are on the page, working as expected. The stylesheet is a bit different, but the colors are right. • The website was extremely laggy. Not the best optimization. • Great job! You secured that oil rig so tight even the crude couldn’t slip past you! • Excellent Job Team 98! I like your teams Oil Rig Status web page, it was neat to know what specific part of the Oil Rig is non operational. • The site is missing the full burgundy color on top of the image. • site cannot be reached