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

FERRIS STATE UNIVERSITY

FSU BULLDOGS

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 43 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	416	27.73%	51
Security Documentation	1043	83.44%	52
C-Suite Panel	1045	83.60%	33
Red Team	1250	50.00%	27
Blue Team	1936	96.80%	12
Green Team Surveys	1482	98.80%	28
Deductions	0		
Overall	**7172**	**71.72%**	**28**

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	416

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

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

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	No
25	No
26	
27.1	No
27.2	No
28	No
29	
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	1043

Strong Points	*Areas of Improvement*
• Network diagram is clear and communicates details well. • Good inventory and network diagram. • The network diagram was very well done. The team also did a great job of identifying relevant services in the asset inventory. • You did a great job writing a complete and well-organized report. The asset list is thorough and easy to understand, and the vulnerabilities you described are realistic and clearly matched to the systems involved. The fixes you proposed make sense and show that you understand why	• Differentiate between mitigation of vulnerabilities and hardening of the system overall with justification for each hardening step. Consolidate CVEs when possible. • The hardening steps need more detailed action plans. • I'd recommend more specific details on the function of each asset in the system overview section. • The "System Hardening" section is full of important information, but it is hard to read because it is a "wall of text". It can be made easier to read by breaking it into smaller

Strong Points	Areas of Improvement
each change matters. The overall report is professional and easy to read. • Network Diagram.	paragraphs, adding short subheadings, and using white space around the numbered list. • The communication skills and critical thinking.

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	1045

Strong Points	Areas of Improvement
• I like how you brought up potential breach of contracts, good buzz words to help draw C-Suites attention. • Overview of risk was good, at the right level and highlighting costs. • Strong point for this entry was most-definitely the operational and business risk. It was clearly defined, prioritized, and understandable for a C-Suite audience. No leads were buried here, it flows cohesively. Additional strong point is the risk reduction strategy. You presented policies and actions that the C-Suite could actively push as a part of organizational change, not falling into just relaying tactical actions that need to be taken for remediation. • Able to identify risk and solution • Good use of video over slides • This was a well-organized presentation with good visual aids that supported your key points effectively. The team demonstrated solid understanding of the topic and delivered information clearly.	• No ties between strategies / recommendations and identified risks. Don't use bar charts/line charts that cross two modalities (e.g. cost/time). • Presentation was over-time. A bit less time could have been spent on the details and incident overview, a greater focus should have been placed on risks and strategies. Recommendations were a bit technical, did require additional funding (could have specified lower-cost changes such as additional cyber training). • explain the costs a little bit more • Discussion of operational and business risk does not exactly match with the content on the slides. • It would be easier to follow long if the their was better alignment. • The risk associated costs should have also been discussed and explained verbally. • For high priority actions, also discuss how associated costs, staffing, were calculated, and more specifics on software and hardware requirements and how timelines were determined. • References on a final slide could provide further context and research areas for viewers. • Overall, this was a good effort. Continue refining your explanations to add a bit more depth and confidence in delivery with small improvements that will make your professional presentations even stronger.

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	125	125	0	250

Whack a Mole		
WAM1	WAM2	WAM3
250	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	461

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
40350.04	89.67%

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
1482

Green Team Survey Comments
• Great job, good luck! • Good job • Good Job • Looking good, keep up the good work! • Nice job Team 43!