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

ST. CLOUD STATE UNIVERSITY

HUSKY HACK PACK

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 50 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	565	37.67%	23
Security Documentation	1153	92.24%	22
C-Suite Panel	865	69.20%	80
Red Team	1500	60.00%	14
Blue Team	1949	97.45%	9
Green Team Surveys	1303	86.87%	21
Deductions	0		
Overall	7335	73.35%	21

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	565

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	No
10.9	No
11.1	Yes
11.2	Yes
11.3	Yes
11.4	
11.5	
11.6	
11.7	
12	
13	No
14	
15	Yes
16	Yes
17	Yes
18	Yes
19	Yes
20	Yes
21	No
22	
23	
24	
25	
26	
27.1	Yes
27.2	Yes
28	Yes
29	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	1153

Strong Points	*Areas of Improvement*
• Presentation and thoroughness of identified vulnerabilities. • great system overview for senior leadership • The team did an outstanding job of identifying vulnerabilities and system hardening strategies. • This report is outstanding: it is complete, accurate, and written with real care. The vulnerability findings are relevant. Your hardening steps are realistic and show strong technical understanding. The document is easy to follow.	• Avoid technical jargon in the overview. Provide list of tools in the hardening section. • Formatting and presentation could be better. For example, get rid of blank pages, structure your system hardening response into sections and bullets, and avoid using full red background color in the vulnerabilities and mitigation section. • The network diagram could use some readability improvements - though the necessary information was there.

Strong Points	*Areas of Improvement*
• The Vulnerabilities section was easy to read and thorough, grouped by systems with vulnerabilities and mitigation techniques well laid out.	• The document is very strong overall. Consider adding a short summary tying together the biggest risk reductions. • The Asset Inventory could have been more thorough.

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	865

Strong Points	*Areas of Improvement*
• Good overview of risks. Recommended hiring additional staff -- sometimes, we can't just get by with existing staff and free/cheap tools, and hiring specialized staff is the only answer. • Great coverage of the risks • Team 50 delivered an exemplary, business-oriented briefing that excelled across all evaluation categories, demonstrating clarity, strategic alignment, and financial prudence suitable for a C-Suite audience. They effectively translated a technical compromise into tangible business risks, including reputational damage, operational disruption, and safety and environmental concerns emphasizing the incident's impact on business continuity and brand integrity, with an estimated operational loss of $123,000 per day. Their strategy was comprehensive, combining a general incident response plan (quarantining, eradication, restoration) with targeted long-term actions such as network monitoring, third-party vetting, awareness training, and formal policy development. Importantly, Team 50 adhered strictly to minimal-funding constraints by recommending free or open-source solutions like Nagios Core and Security Onion, providing strong justification for each recommendation and aligning every action with identified risks. The presentation was professional, well-structured, and visually consistent, reinforcing the team's credibility and overall exemplary performance. • Clean slide design.	• Recommendations and strategies don't clearly tie back to identified risks and incident. • Identified risks were not directly addressed later on • Equal Participation: While three members (KJ, Griffin, and Liam) presented, and all six members (including Colin, Carl, and Dustin) were mentioned, but roles were not mentioned time. To achieve the highest score of Exemplary, the team should aim for a more balanced distribution of roles. Additionally, they should explicitly mention and acknowledge the specific contributions or roles of the non-presenting members, such as research, data analysis, slide design, or strategy development to clearly demonstrate full team collaboration and ensure all members receive visible recognition for their work. • The role and tasks completed by students not presented should be included. • Good work quantifying the risk financially. • More details on response strategy and strategic actions needed: staffing, software, hardware, timing, and cost. • Longer-term outlook: should list associated costs, and timelines. • felt the financial impact to the business would value more substantiation than the 2 stats and how they were positioned if you want to make it easier to make change / justify cost, whatever it is. Also, didn't cover cost of training & additional ICS Engineer, or headcount availability. Felt the solution presentation was too techy, talking about

Strong Points	*Areas of Improvement*
• well presented and well coordinated as a team. • Strategy addresses identified risks. Recommendations are clear on why they would prevent the risk from reoccurrence.	onions etc. Also Social Engineering Training isn't going to prevent an authorized 3rd Party engineer on an oil rig from plugging in a device that been infected. • Risks were addressed in isolation

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	250	0	250	0	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
1455	494

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	23	26	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
43219.97	96.04%

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
1303

Green Team Survey Comments
• Site looks good, but I had no access to the 'Admin Dashboard'. I could log in, but it only returned me to the main screen. • There is no User 'Management' button. • footer not included on homepage. • Excellent work! • good job • the headers are lil bit uneven spaced- but looks ok • Looks perfect! • Good job • site cannot be reached • site can't be reached • site cannot be reached