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

UNIVERSITY OF NORTH GEORGIA

UNG HACKHAWKS BLUE

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 91 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	510	34.00%	32
Security Documentation	738	59.04%	87
C-Suite Panel	871	69.68%	79
Red Team	1250	50.00%	27
Blue Team	1886	94.30%	25
Green Team Surveys	1397	93.13%	37
Deductions	0		
Overall	**6652**	**66.52%**	**37**

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	510

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

1	Yes
2	
3	
4	Yes
5	Yes
6	
7	
8	No
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	No
13	
14	
15	Yes
16	Yes

17	Yes
18	Yes
19	Yes
20	Yes
21	Yes
22	
23	
24	No
25	Yes
26	
27.1	No
27.2	
28	
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	738

Strong Points	*Areas of Improvement*
• Demonstrates good technical understanding and traces an actual attack chain clearly. • Excellent depth and clarity in the Vulnerabilities and System Hardening sections: findings are host-specific, each line includes an appropriate mitigation, and the hardening narrative ties root-cause to concrete corrective actions across AD, Web, Public DB, Task, HMI, and PLC in leadership-appropriate language. • Good job on being able to explain everything in a simplified manner.	• Streamline explanations and link actions directly to risk reduction. • Elevate the network diagram to "exemplary" by adding a clear legend, labeling subnets/roles, and explicitly showing logical interconnects AD/DNS queries, web - DB dependencies, and ICS HMI - PLC flows so readers can understand relationships at a glance; ensure one-to-one consistency with the asset inventory • The network diagram needs to be more elaborated and describe what the

Strong Points	*Areas of Improvement*
• great work making the connections in the network diagram	connections mean and what the machines are. • Format for System Hardening can be improved using bullets and sub-section titles. In a business setting, people prefer bullet points over large blocks of texts.

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	871

Strong Points	*Areas of Improvement*
• the costs and risks • Very well explained business impact with dollar loss discussion and well designed slide. • Good work referencing the C2M2 and NIST Cybersecurity Framework. • good detail on financial impact, • Big fan of adding references and being clear on the use of AI. • Mentioning of NIST and C2M2 Compliance models! Loved the flow, data, timeline, enthusiasm like a real conversation and overall incident into business terms. References to data and cost analysis was perfect! Franchise value and licensing to operate, stakeholder confidence, charts and data was excellent models of real world use cases. • Remediating the Compromise Timeline Priority	• better allocation of time per member • Did not include strategies to reduce business risk. • Did not include high priority recommendations. • maybe too much on the financial impact at the day cost, but showing the week / month actual costs that will create impact makes sense. • The actions are great but does not follow what we are asking for. • If you are going to discuss Indicators of Compromise / IOCs then you should reference MITRE ATT&CK framework steps

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
125	0	125	0	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
1475	411

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
35954.96	79.90%

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
1397

Green Team Survey Comments
• When I log in I did not see the admin dashboard which says I wont when I log in but the next question is check the users but there is no user management. • Good job, might want to put footer on home page

Green Team Survey Comments
• Site looks good, but I had no access to the 'Admin Dashboard'. I could log in and there was no 'Admin' button, but it only returned me to the main screen. • "Normal User: Able to get Admin on header drop down but access to User Admin was blocked ... Good job! No footer on Home Page." • Excellent work! • web.blue0091.cfc.local refused to connect.