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

UNIVERSITY OF NORTH CAROLINA AT CHARLOTTE

49TH SECURITY DIVISION

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 3 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	709	47.27%	12
Security Documentation	1071	85.68%	45
C-Suite Panel	970	77.60%	56
Red Team	1375	55.00%	22
Blue Team	1851	92.55%	30
Green Team Surveys	1363	90.87%	19
Deductions	0		
Overall	**7339**	**73.39%**	**19**

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	709

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

1	Yes	10.7	Yes	17	Yes
2	Yes	10.8	Yes	18	Yes
3	No	10.9	Yes	19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6		11.3	Yes	22	Yes
7		11.4	Yes	23	
8		11.5	Yes	24	No
9	No	11.6		25	Yes
10.1	Yes	11.7	Yes	26	
10.2	Yes	12		27.1	Yes
10.3	Yes	13		27.2	Yes
10.4	Yes	14		28	Yes
10.5	Yes	15	Yes	29	Yes
10.6	Yes	16	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	1071

Strong Points	*Areas of Improvement*
• Strong technical depth combined with a table of contents up front allowing for executive decision makers to quickly evaluate the information, if needed. Time is of critical importance as the most valuable, and most constrained, resource. • Good network diagram. • Overall the security documentation was strong and covered the requirements. In a few places went above and beyond. I did like the list of open ports by host. I also liked the logical join in the Network Diagram	• Improve formatting of the steps to pursue system hardening. Consider applying a prioritized number schema to allow for holistic risk management. • The team did not follow the template for documentation, making it difficult to judge. • The System Overview could have been more holistically focused with respect to the business, which would appeal to the C-Suite audience. A stronger justification for the System Hardening, the why is this being done, included.

Strong Points	Areas of Improvement
between AD/DNS and DB, along with the DNS resolver. • Very clean & easy to read, excellent detail in the vulns	• Would have been great to see CVEs cited for the vulns and some type of EDR with centralized logging in the system hardening section.

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	970

Strong Points	Areas of Improvement
• Good summary of risks and connections between operational and business risks is clear, including financial risks. Plan is focused on immediate concerns but does make connection to previously noted risks. • The speakers were well rehearsed. Also, the risk section was particularly effective in referencing financial data. • good content • Correct use of the time and every team member was acknowledge to participate. Some of the risks were well identified and strategy looks promising and could be further developed. • Risks Related to Operational and Business Concerns (30%): The presentation provided a clear summary of both business and operational risks. The team clearly identified how these risks affect the company's bottom line (finances), quantifying the trade-off by contrasting the $130,000 daily loss from halting production against the ""millions or billions of dollars"" in costs associated with property damage, environmental lawsuits, or ""grave harm to personnel"" that previous oil platform incidents have caused. • Strategy to Reduce Risks (30%): The team provided a complete strategy. This included a comprehensive response plan (four immediate actions: halt production, identify/close channel, remove unauthorized systems/software, validate system integrity) and crucial long-term policy updates. These long-term actions included ceasing engagement with the specific contractor, re-evaluating vetting processes,	• Visuals would help your audience follow the key points. Missing clear strategy statement for reduction of risks long-term yet offers several recommend actions. • While the presentation was overall effective, the use of slides or another visual aid would help engage the audience more. Also, further discussion of the cost of some suggestions would improve the presentation. For instance if we need to validate all readings with another measurement technique, how much might this cost? • no visual aids and did not look rehearsed • The presentation was reasonable but was hard to follow, since no visual aids were used. It wasn't clear how the process of risk-mitigation-recommendations was going to be follow to prevent further atttacks. • Professional Appearance (Dress Code): The team received an Emerging (1) score in the Quality of Presentation category because two of the presenters wore track wear jackets. The rubric specifically defines an ""Emerging"" score as having an ""Inappropriate dress code, the team is not dressed for a work environment,"" which is a mandatory requirement for a C-Suite briefing. For future C-Suite presentations, all team members must be dressed professionally, as expected for a work environment. • Visual Aids and Professionalism: The team relied solely on presenting without visual aid. To achieve higher scores (Proficient or Exemplary) in the Quality of Presentation category, the team should incorporate

Strong Points	*Areas of Improvement*
and implementing network device approval functionality. • High Priority Recommendations (30%): The team successfully presented four high-priority actions. They provided complete and consistent reasoning for these actions, particularly justifying immediate production halt as a necessary step to prevent catastrophic financial and physical damage. Crucially, the recommendations adhered to the financial constraint requirement by suggesting the use of only free or open-source tools (such as Grey Log or the Elk Stack) for monitoring, requiring ""at most a minimal level of additional funding"" • The presenters obviously put a lot of work into the production of the video and did a great job explaining the content. The summary at the end, including details on the introduction of the vulnerability was a good add and helped round out the presentation.	visual aids, slides, or other materials to ensure a ""consistent, professional appearance"" and avoid relying solely on presenting verbally. Visual materials can also aid the C-Suite in following complex information. • Presentation to the Full C-Suite: While the technical content was outstanding, ensure the language used is suitable for all members of the C-Suite, not just the technical audience (e.g., the CIO or CTO). Technical details and jargon should be avoided, or carefully translated, to focus on the business impact and consequences, which helps maintain the ""Exemplary"" standard for suitability across the leadership panel • It was unclear whether there were additional team members besides those who spoke throughout the video. No visual aids were used, making this difficult for visual or non-auditory learners to follow.

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	125	0	250	125	0	250

Whack a Mole		
WAM1	WAM2	WAM3
250	250	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
1465	386

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	25	27	27	26	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
33799.60	75.11%

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
1363

Green Team Survey Comments
• No issues. Great Job!
• Good job Team 3! Good luck defending your oil rig!
• Good job
• Although technically all correct, the formatting of the header needs to be fixed.
• Everything is in place. Good job!
• Good work! All intended areas are still accounted for within the website and no issues locating anything per the requirements.
• Great job! You secured that oil rig so tight even the crude couldn't slip past you!
• Nicely done!
• web.blue0003.cfc.local refused to connect.
• Site is down