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

UNIVERSITY OF FLORIDA

DARTH GATOR

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 37 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	696	46.40%	14
Security Documentation	1229	98.32%	2
C-Suite Panel	1041	83.28%	36
Red Team	1500	60.00%	14
Blue Team	1753	87.65%	45
Green Team Surveys	1278	85.20%	10
Deductions	0		
Overall	**7497**	**74.97%**	**10**

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	696

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		10.9		19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	Yes
6		11.3	Yes	22	
7		11.4	Yes	23	
8	No	11.5	Yes	24	No
9	No	11.6	Yes	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	
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	1229

Strong Points	*Areas of Improvement*
• Great job hitting the major areas of the rubric. • All vulnerabilities are identified and mitigated with strong technical justification. • The document was thorough. • Covered great amount of details with clarity and looking good to present. Overall great effort by the team specially in the vulnerability listing and system hardening section. • You delivered a well-structured and accessible security summary that would resonate strongly with a C-suite audience.	• The tools used section would be better placed in another section, such as the system hardening one, rather than right below the network diagram. Also, breaking up the system hardening section into subsections, for better readability, as well as using black font instead of gray would be an improvement (keep in mind the senior leadership audience). • Divide longer sections and tables for easier reading. Use more headings and visual breaks to improve clarity. • Avoid gray fonts in the future.

Strong Points	*Areas of Improvement*
The clarity and organization of your content showed real discipline in how you approached executive-level communication.	• The network diagram can be improved and unwanted section like 'tools used' can be avoided. • You already communicate at a level that works well for a C-suite audience. One small enhancement that could make your work even stronger is adding just a bit more technical context behind some of your high-level point. You're very close to an ideal balance, and a small amount of added depth will elevate an already well-crafted summary.

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	1041

Strong Points	*Areas of Improvement*
• OSHA fine, 3rd party vetting, 1 week delay were not mentioned by other teams! Excellent format for your high priority slides. • There truly was an organic component to both the visuals and the speaker handoff here. You clearly are team that tried to connect and collaborate and this showed as you segued from one person to the next and from one slide to the next. You even all aligned your virtual backgrounds so as to create a homogenous and unified offering. Your teamwork and collaboration are truly fantastic! • Good overview of risks with explicit $ values. Like the breakdown of both short and long responses with examples of products and implementation timelines. • Clearly outlined business risks and operational impact following an industrial control system compromise, with direct ties to reputation, safety, and production. • Fantastic submission. I loved how you led with network segmentation as the highest priority recommendation and all team members participated • Your high priority recommendations were clearly stated with reasons why they would reduce risk.	• Small hyperlinks - omit, distracting; can be emailed to audience later. Cybersecurity quote on next to last slide is not appropriate for C-Suite. They are your bosses - instead summarize by "your cyber team is standing by to immediately implement these recs and will have __, __, and __ fully complete within __ days. The SOAR will take 2 years to fully implement. Explain that "training SOAR uses machine learning to recognize normal and abnormal conditions." Instead of "Thanks" on final slide, say "We are available to answer your questions." Keep 1st speaker fully in frame (his hair was chopped off). While explaining safety of life, also emphasis no destruction of a very expensive oil rig. • The content in the presentation, unfortunately, felt spartan. There was only a single long term solution offered: SOAR, and while this orchestration is a fantastic recommendation, no SOAR is a cure all for all cybersecurity threats, I would even argue that much of what Shuffle here does has quite a bit of overlap with Elasticsearch, while missing many other attacks like insider threats, social engineering, or supply-chain attacks—like the one that hit

Strong Points	Areas of Improvement
	Abyssal Pearl. As such, there needs to be a more comprehensive solution offered here. • On a related note, the Risks of Inaction slide that was tacked on at the end didn't land for me. If you want to scare senior leadership into action, this is something that should be at the start of the presentation to get your audience to sit up and listen. Here at the end, it seems like you are trying to connect and then walking away just as you have our attention. • There was no tie between your risk reduction strategies and the risks you identified. • Recommendations could be more quantified (financial analysis of prevention costs versus risks) and tailored to Obsidian Rift Energy's specific environment. • I don't think it really could be, you all took the time to dress up nice and make a really good video, excellent work • Your risks need to be more thoroughly explained before you discuss their effects on the bottom line.

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	250	0	125	250	0	125

Whack a Mole		
WAM1	WAM2	WAM3
250	125	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
1465	288

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)
26	27	27	26	26	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
25218.80	56.04%

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
1278

Green Team Survey Comments
• no footer on homepage
• No footer on the main homepage.
• Footer missing on home page
• footer missing from main page
• Good job.
• Nice Job Team 37! Good luck!
• Looks great!
• "Slight variation of home page --- however meets criteria for marking true
• The oil rig is sized oddly. The water would be viewable usually and is not scrollable."
• website is down
• Site is down