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

TRITON COLLEGE

THE SOCIETY

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 87 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	310	20.67%	74
Security Documentation	835	66.80%	80
C-Suite Panel	1045	83.60%	33
Red Team	500	20.00%	70
Blue Team	1781	89.05%	41
Green Team Surveys	1205	80.33%	63
Deductions	0		
Overall	**5676**	**56.76%**	**63**

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	310

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

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

10.7	Yes
10.8	No
10.9	
11.1	Yes
11.2	Yes
11.3	Yes
11.4	Yes
11.5	Yes
11.6	No
11.7	Yes
12	
13	
14	
15	Yes
16	Yes

17	No
18	Yes
19	Yes
20	No
21	No
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	835

Strong Points	*Areas of Improvement*
• Very complete asset inventory. • great job describing their process for securing accounts, updating systems, and setting strong password and patching policies. • Extensive asset inventory.	• Lacks logical connections in network diagram. Would have liked to see more than "Reverted to Default State" as mitigations - what was default? • Vulnerabilities section was vague about impact and had an in appropriate technical level for the audience. Many identified items were subjective as to whether they were vulnerabilities or not. System inventory could have been organized better to make it easier to identify systems, instead of dropping in a row for each open port. Most

Strong Points	*Areas of Improvement*
	actions in the hardening section were remediation tasks, not hardening. • Adding short summaries or tables at the start of each section would make the report easier to navigate for busy readers. • Consider closer attention to formatting and polish. Senior leadership often need concise text that is easily read.

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*
• Nice smooth start. Very good slides. • Strengthen and Prevent, Monitoring Tools, Knowledge of the content and the cybersecurity tools • Very well reasoned out, and aspects were tied back to business concerns and bottom line. The presentation and visuals were well done. • Covered and outlined business risks and operational impact following an industrial control system compromise, with direct ties to reputation, safety, and production. • Presentation slides were well done with no extra information that wasn't needed. • The team provided good information and showed a clear understanding of the topic. The presentation flowed well, and your explanations connected the material to the overall objectives effectively.	• Incident Response slide - graphic doesn't match, recommend an oil rig related graphic. Also, "we can not be certain" would be better as "we are thoroughly investigating". Risks of Inaction slide - comes across as a negative to the C-Suite. Instead, show them how to recover. Financial impact - give $ amounts after some research. Aramco case study should not be discussed - talk about what it takes to fix Abyssal Pearl. Step 1/2/3 slides do not show the costs for each step or time needed. Only 1 of the 3 tools had a cost provided verbally. If tools are free, put that on the slide "cost $0". No discussion about screening contractors. • Nothing else except expected cost to the organization with implementation of security tools and the roadmap • The presentation was quite long. • Recommendations could be more quantified (financial analysis of prevention costs versus risks) and tailored to Obsidian Rift Energy's specific environment. Vendor management and risks could be more specific. • The plan overall is great but does not target the specific points that were asked for. Remember what the goal is and the target audience. • Keep building on this foundation together by adding a bit more detail to your analysis and maintaining confident, consistent delivery

Strong Points	*Areas of Improvement*
	as a team. You're developing strong collaborative and presentation skills that will serve you well professionally.

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	0	0	0	125

Whack a Mole		
WAM1	WAM2	WAM3
125	125	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
1330	451

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)
0	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
39446.56	87.66%

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
1205

Green Team Survey Comments
• Good job! • Once again there was no user management button. • Home Page - Footer is cut off, Nav bar is not aligned, Login - Footer is in the login container. • rig-status page didn't come up • Oil rig status page was unable to load • The navigation bar wasn't formatted from left to right, good luck! • Webpage did not load. Error message: Internal Server Error • Unable to access site - Internal Server Error: Illuminate\Database\QueryException = Connection Refused • red user added • logos do not look centered • web.blue0087.cfc.local took too long to respond. • 5:51 This site can’t be reached