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

LIBERTY UNIVERSITY

CTRL+ALT+ELITE

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 18 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	482	32.13%	35
Security Documentation	1215	97.20%	6
C-Suite Panel	1208	96.64%	1
Red Team	1750	70.00%	8
Blue Team	1611	80.55%	57
Green Team Surveys	1456	97.07%	6
Deductions	0		
Overall	**7722**	**77.22%**	**6**

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	482

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

1	Yes
2	
3	
4	
5	
6	
7	
8	No
9	Yes
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	
11.1	Yes
11.2	Yes
11.3	Yes
11.4	Yes
11.5	Yes
11.6	Yes
11.7	Yes
12	No
13	
14	
15	Yes
16	Yes

17	Yes
18	Yes
19	Yes
20	Yes
21	
22	
23	
24	
25	No
26	
27.1	Yes
27.2	Yes
28	Yes
29	No
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	1215

Strong Points	*Areas of Improvement*
• Very strong justifications and thoroughly capturing details in every section. Good idea to set up a SIEM to help with monitoring • The documentation as a whole was great. • The team did an outstanding job with their documentation. They particularly shined in identifying vulnerabilities and in their system hardening strategies. • The report was clear, fairly concise, and content was solid. • The system overview used effective and concise language that is appropriate for senior leadership	• Some minimal errors in asset inventory port list, but not enough to lose points • Avoid jargon for senior leadership. • Some services were not accounted for in the asset overview (but not enough to affect scoring). • The formatting could have been clearer to delineate elements and highlight important parts. • Senior leadership might not understand some technical terms. Consider how technical content might be made more

Strong Points	*Areas of Improvement*
	accessible to an audience without your expertise

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	1208

Strong Points	*Areas of Improvement*
• Very professional and good research conducted for the presentation • Like the slide layout, easy to follow and got my attention to key spots. • Stunning work. Many teams get bogged down in technical minutiae that C-suite executives don't need to hear, but this presentation avoided that pitfall. It was concise, focused on strategic rather than purely tactical recommendations, and stayed well aligned with the original incident and associated risks. The team emphasized policy and process improvements, including options that can be implemented using FOSS tools. Props for the introduction of a risk management framework recommendations. Financial risk was clearly considered throughout and drove a lot of recommendations. The presentation was polished, balanced across all sections, and delivered with impressive clarity. Fantastic job. • Thorough understanding of regulatory impacts and financial risks, and a stepwise NIST framework methodology for risk management. • Clean and professional presentation materials. Including relevant documents and references helped to set this presentation apart. Nice work including the cost of internal labor and infrastructure - this is often overlooked. • It was great to see so many sources & references, excellent work on the research side!	• Strategy and recommendations were a response to the incident and not a direct correlation to the business risks. Reasoning and cost of high priority recommendations were unclear • This is more regarding order, but it may be beneficial to clearly call out the consequences listed in the conclusion slide closer to the presentation segment where you discuss risks and impacts. Worker health and safety is a significant concern that was covered on the conclusion slide, but it may be beneficial to make that more prominent earlier on as well. • Vendor management could be more specific, emphasizing IoT/OT supply chain risks, and recommendations could be linked to measurable outcomes. • It's difficult to identify areas of improvement. This was one of the better presentations. • The costs felt a little unrealistic, it would have been great to see a better breakdown of how many hours of time implementing the new security controls is projected to take

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	250	250	125	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
1485	126

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	27	27	27	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
11062.63	24.58%

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
1456

Green Team Survey Comments
• 'Red' admin • 'Red' admin • Admin tag missing. • missing user • The navigation bar on the homepage says Admin instead of Login. • Nice Job Team 18!