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

UNIVERSITY OF DENVER

SOC SQUAD

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 82 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	353	23.53%	65
Security Documentation	1012	80.96%	57
C-Suite Panel	919	73.52%	69
Red Team	375	15.00%	77
Blue Team	1594	79.70%	61
Green Team Surveys	1106	73.73%	72
Deductions	0		
Overall	**5359**	**53.59%**	**72**

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	353

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

1	No
2	
3	No
4	
5	Yes
6	No
7	No
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	Yes
11.1	Yes
11.2	Yes
11.3	Yes
11.4	Yes
11.5	Yes
11.6	Yes
11.7	Yes
12	
13	No
14	
15	Yes
16	Yes
17	No
18	Yes
19	Yes
20	Yes
21	
22	
23	
24	No
25	
26	
27.1	No
27.2	
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	1012

Strong Points	*Areas of Improvement*
• Good detail provided for the asset inventory, network diagram, and vulnerabilities sections. Great work! • "This report demonstrates strong technical quality and accurate findings. The mitigations are realistic and supported by evidence. • The document's structure and formatting are clean and consistent." • Vulnerability and mitigation coverage is comprehensive and justified for every host. • Known mitigations was comprehensive.	• Areas for improvement include enhancing the detail in the system overview section by providing definitions and the purpose of each system. Additionally, the language should be adjusted to specifically target senior leadership. Limit or provide context for technical jargon such as AWS, AD/DNS, DB, HTTPD, RPC/NFC, SSH, SMTP, IMAP, SMB, ICS, HMI, PLC, and TCP. Furthermore, the system hardening section can be strengthened by introducing at least four comprehensive hardening steps with justifications. The current section tends to

Strong Points	*Areas of Improvement*
- Extensive asset and vulnerability enumeration	repeat mitigations from the previous section with minimal justification. - Severity or CVE identifiers should be added for each vulnerability to establish priority. - Including a brief risk summary at the start of the section would make it more executive-friendly. - Break up long tables and dense blocks for better readability. Add more headings and visual separation as needed. - System overview didn't discuss purpose of system. Asset inventory was missing services, ports, and no OS was listed for the web server. - Consider senior leadership audience more closely. Think of ways to concisely make your systems and recommendations relevant to the rest of the business.

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	919

Strong Points	*Areas of Improvement*
- The operational and business risks were well thought out. - Addressed cost of hiring new staff - well thought out and laid out slides. - Presentation is easy to follow and the graphics are helpful. - Operational and Business Risk chart was very clear. Mention of Reputational - Damage and Regulatory Penalties was a plus. Mention of ICS - Systems and Forensic Evidences (i.e. logs) was a plus. Phishing and MFA were two areas of training that would alleviate Human Error. - Containment strategy is easy to follow.	- It would have been helpful to specify where the financial information verbally mentioned on the 'risk' slide came from. At 1:47, how did you calculate that a day can cost multiple millions of dollars– where is this number coming from? - Also, there was no description of cost associated with high priority recommendations, such as how much the 'cyber hygiene training' program you described would cost. - Last, some of the high priority recommendations seemed more long term but a more explicit long term strategy should have been detailed." - Strategy and high-priority recommendations weren't tied back to risks. - again focusing on employee password training but I believe that contain the incident that was caused by an authorized contractor plugging in an infected device wouldn't be addressed by this, as with MFA as the worker was authorized.

Strong Points	*Areas of Improvement*
	• There are some slides that have too much writing and could just be a few bullet points instead. • Please explain how you will apply principal of least privilege and what unnecessary applications will be updated or removed. How will you back up your log files? How will you monitor your ports and implement a network policy that will make the attack surface smaller?

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	0	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
1285	309

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)
16	27	0	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
27022.51	60.05%

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
1106

Green Team Survey Comments
• Good job • 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. • The company name in the Header is wrong. The footer is not on every page. There are other formatting and spelling errors. • check your headers and admins! • Wrong background image, Admin buttons are orange (should be burgundy), red is an admin • Too many admins • company name misspelled, yellow buttons, Red Admin added, additional users, logos not see through • too many admins • Great Job Team 82! • Energy is spelled wrong (it is currently energi), red is currently and admin • your header is incorrect and so are your logos, not all site accents are the correct color, and you have an extra admin. • 5:45 This site can't be reached • 5:54 This site can't be reached • Forbidden You don't have permission to access this resource. Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request."