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

BRIGHAM YOUNG UNIVERSITY

BYU COUGARS

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 13 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	533	35.53%	25
Security Documentation	1122	89.76%	29
C-Suite Panel	1078	86.24%	27
Red Team	1625	65.00%	13
Blue Team	1909	95.45%	18
Green Team Surveys	1149	76.60%	13
Deductions	0		
Overall	**7416**	**74.16%**	**13**

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	533

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	
6	No	11.3	Yes	22	
7	No	11.4		23	
8		11.5	Yes	24	No
9		11.6	Yes	25	Yes
10.1	Yes	11.7		26	
10.2	Yes	12		27.1	No
10.3	Yes	13	No	27.2	No
10.4	Yes	14		28	Yes
10.5	Yes	15	Yes	29	No
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	1122

Strong Points	*Areas of Improvement*
• The vulnerability list was extensive. • The team did a great job of identifying vulnerabilities and other configuration issues. • Tables and diagram were well done. It was well written in clear language. • Detail documentation • The report was clear and concise, with solid content.	• The hardening steps were great but strong justifications were not provided. Vulnerabilities were not provided for the PCL and HMI systems. • The team's system hardening recommendations are overly technical for a C-Suite audience. • The System Hardening could be a bit better organized to make it easier to follow. • The formatting could have been clearer to delineate elements and highlight important parts.

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	1078

Strong Points	*Areas of Improvement*
• Overall cost/risk analysis and affect of investments, citing external sources • Good work on quantifying the risks in monetary and repetitional values. The Risk Reduction Strategy by terms: Stabilize->Secure->Verify->Sustain was a good way of communicating the information in a memorable way. Good work on the final reference slide. • Presentation as easy to follow. Your images didn't get in the way of being able to see or follow your slide. • their alignment of technical situation to business risk & impact in understandable non techy jargon was strong • Good job quantifying the impacts of incidents relative to the concerns of the C-suite. • I like the strategy categories.	• Risk reduction strategy is purely sequential, and some early steps are more tactical than strategic. • Additional recommendations to consider: back ups, IDS/IPS, patching vulnerabilities, etc., also consider how these would be prioritized with your recommendations and consider cost/time to implement, etc. • For strategies and recommendations: also discuss will this require additional staffing or contractors, software or hardware purchases, timelines. • Would also recommend a list of software, hardware specifics for further consideration • Could have been more professional dressed. Risk reduction strategy could have listed tool and timeline. • Opening as ""we researched the cyber event"" & nothing about being ""the Incident response Team"", but identified their team correctly for scoring purposes. • some other videos had even more $$ impactful stats more likely to grab the C Suite attention; but without deep research I don't know how factual. However, knowing first hand the mixed risk appetites in reality, Total Cost of Impact including monetizing reputation loss is more likely to make easier to get them onboard fully re Cyber posture. • You covered impacts during your discussion of risk. That is only half the calculation of risk. • How does the risk reduction strategy reduce the risks you talked about?

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
250	0	250	0	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
1455	454

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	24	27	27	25	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
39727.08	88.28%

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
1149

Green Team Survey Comments
• footer not visible on home page • Footer is not on the bottom of the home page. • check footer position on homepage • red user added • homepage footer too high position • Great job! • Excellent work! • did not load • Website unable to load • Site won't load • Perfect • site cannot be reached • Site is down