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

SOUTHERN UTAH UNIVERSITY

SUU THUNDERBIRDS

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 83 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	448	29.87%	43
Security Documentation	945	75.60%	69
C-Suite Panel	1109	88.72%	14
Red Team	500	20.00%	70
Blue Team	1990	99.50%	1
Green Team Surveys	1352	90.13%	49
Deductions	0		
Overall	**6344**	**63.44%**	**49**

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	448

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

1	No	10.7	Yes	17	Yes
2		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	Yes	23	
8	No	11.5	Yes	24	
9	No	11.6	Yes	25	
10.1	Yes	11.7	Yes	26	
10.2	Yes	12		27.1	No
10.3		13	No	27.2	No
10.4		14		28	Yes
10.5	Yes	15	Yes	29	
10.6	No	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	945

Strong Points	*Areas of Improvement*
• Overall, great work! The sections on asset inventory and system hardening were particularly well done. • Very complete asset list. • The network map was well laid out and easy to read. • Good job documenting plenty of vulnerabilities! • Covered great amount of details with clarity and looking good to present. Overall great effort by the team.	• The known vulnerabilities section can be improved by using appropriate language for better understanding and decision-making targeting senior leadership. • System overview does not describe the OT system at all. Missing good mitigations for most vulns. • The asset table was hard to read, there are better ways of listing redundant information so the reader can see what is going on. • Keep your hostnames consistent. Try not to only have a version or patch name as your

Strong Points	Areas of Improvement
	mitigation. When you list CVEs, try to also describe the vulnerability. • N/w diagram can be more clear.

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	1109

Strong Points	Areas of Improvement
• I did appreciate the slide that provided a high level overview of an attackers tactics, techniques, and procedures. They nicely underpinned the conversation surrounding containment, risk-reduction strategies and the high priority recommendations. Complete and consistent reasoning was given for all actions, reasoning was provided for why recommendations would reduce risks and a note that the actions would require little to no funding. Additionally there was a highlight on the consequences of taking no action, this was very well done and flowed smoothly and really supported the overall argument as well. • I liked that several folks spoke and the team was introduced at the beginning. I liked the overview of the attack approaches to educate C-suite. I especially liked the Business Continuity Plan during the response. • The typical attack order was a good addition to help those in the c-suite with less familiarity get an understanding of what they may be facing and how this may have happened. The executive summary was done well also, giving a clear ending to the presentation and a summary of key information for the c-suite. Overall, the presentation was strong and the information was clearly presented. • The summary was good, and the call to action was very strong. The indication of being more resilient and more profitable was very nice. • Giving knowledge of how attack patterns work before giving your strategy to reduce	• The team was dressed appropriately and prepared a professional slide deck. Unfortunately, parts came across as not well rehearsed or poorly understood which detracted from the quality of the presentation. The conclusion was also extremely abrupt and could be improved upon to enhance the professionalism of the overall presentation. The team did provide a summary of risks to the organization but did not adequately address how they impact the financial bottom line. • I did not deduct points for this, however ICS stands for industrial control systems, not internal control systems. • While the solutions presented were well thought out, they seemed to be very IT focused. I realize this is the cyber response team, but C-suite needs to know how this fits into the overall business. A more holistic approach to solutions could be considered including policy, workforce, physical security along with a cost benefit analysis. It wasn't clear if the staffing recommendations were to hire new staff or to reallocate existing staff to the cyber response team, both of which would incur a financial cost. • Further practice with public speaking/presenting will push this group's presentation above and beyond. • You may not need to go into detail on how most cyber attacks happen at the C suite level. • Remember that each action you take will have a cost that the C-Suite would like to know before they have you do that action. Yes, overall each action will save money but

Strong Points	*Areas of Improvement*
the risks was different and could be very beneficial. • Both speakers were easy to understand. Professional slides. • Good work discussing the cost of inaction.	they would also want to know which ones would save the most and cost the least. • Include speaker names under their videos. Operational & Business slide doesn't match spoken "safety, production, brand reputation". Typical attack slide - attempt to educate C-Suite - you should stick to the actual attack. High-priority actions - use #s (1, 2, 3, 4) as bullet point symbols. Staffing - unclear if these are current employees or new hires - this matters. Tools cost not SHOWN on slide. Open source may not be understood by C-Suite members. No timeline given, no costs shown. General classroom discussion points made that are not focused the case. "Have a good day" - not how you want to end. Instead, "we are available to answer your questions." • Operational & Business Risks: Speaker discussion doesn't align exactly with the slide content. • Risks should be quantified financially. • Typical attack order and techniques slide and discussion is not required. This time could be used for required discussion. • Containment and risk reduction strategies and high-priority actions should include costs, and hardware and software requirements, and timelines. • Speaker volumes are not uniform.

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	0

Whack a Mole		
WAM1	WAM2	WAM3
125	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
1475	515

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	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
49362.37	109.69%

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
1352

Green Team Survey Comments
• The footer on the home page needs to be lower, and there is no footer on the login page.
• Good Job Keep It Up
• Nice job! Everything's included and mostly well done!
• users added
• Nice Job Team 83!
• website is down
• 5:54 This site can't be reached