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

DEFENDING U.S. ENERGY INFRASTRUCTURE

UNIVERSITY OF VIRGINIA

CNS@UVA

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 16 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	697	46.47%	13
Security Documentation	882	70.56%	75
C-Suite Panel	1031	82.48%	38
Red Team	1500	60.00%	14
Blue Team	1887	94.35%	22
Green Team Surveys	1176	78.40%	27
Deductions	0		
Overall	**7173**	**71.73%**	**27**

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	697

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

1	Yes
2	
3	
4	Yes
5	Yes
6	No
7	No
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	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	No
13	No
14	No
15	Yes
16	Yes

17	Yes
18	Yes
19	Yes
20	Yes
21	Yes
22	Yes
23	
24	
25	
26	
27.1	No
27.2	Yes
28	Yes
29	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	882

Strong Points	*Areas of Improvement*
• Good, comprehensive network diagram. The document read well. • Good list of vulnerabilities and asset inventory • The team did a good job of identifying assets and services. • Covered great amount of details with clarity and looking good to present. Overall great effort by the team. • The overall presentation.	• No vulnerabilities were listed for the HMI. It may help in future efforts to double-check that some items aren't unintentionally left off of long lists. • the hardening needed some work. • some key vulnerabilities were not documented. The system hardening section seemed to be more of an extension of vulnerability mitigation, rather than a high-level strategy to improve the security posture of the system. • Table and page formatting for more readable purpose can help.

Strong Points	Areas of Improvement
	• Technical skills and strategic thinking abilities.

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	1031

Strong Points	Areas of Improvement
• Called for updating contractor policies - few teams did this. (Companies use contractors to reduce their staffing costs - a necessary evil.) Clean slides. • great job focusing on $ for business risks • I enjoyed the Cost slide and the Recommendations • Good job quantifying impacts to incidents. Your strategies are long term and high level, which is what we want. • The team provided an in-depth analysis of the business risks that directly impact revenue, along with compliance risks that could lead to additional financial losses. The clear breakdown of responsibilities at the end, giving each member credit for their contributions, was also a very nice touch. • The presentation was clean and professional and I thought having the video of the team presenting was a nice touch.	• Initial speaker was very quiet. Label speaker names under their video. Background slide: only showed 3 points but discussed 5. Team only recognized by name at the very end - put their names on the slide. Risks slide: $120k or $130k per day - speaker said both. Too many uses of "also". Costs - use $k or $M for costs to reduce # of zeros. You didn't prioritize your recommendations nor provide cost estimates. Don't finish with "Thank you" but instead give the C-Suite a recommendation for them to make a decision today. Lots of slide white space with small font - increase font!!! No discussion on performing system diagnostics or forensics NOW - should be #1 strategy. • use more visual aid, not just text • Need some more specific examples on the Recommendations slide as to how they propose to investigate or search. An example of investigating the network would be: "We suggest monitoring the network and having visibility into key assets using a NIDS or Network Intrusion Detection System like Snort or a Cisco Firewall." • You listed impacts of incidents, but not address likelihood, which is the other factor in risk. • Specify how your strategy reduces the risks you specify. If you build resilient ICS, how does that lower the risk you specify? Does it reduce the likelihood of incident? Does it reduce the impact? • How much will the high priority recommendations cost? How will they reduce your risks? • The presentation content aligned well with the rubric and was well organized. However,

Strong Points	*Areas of Improvement*
	improving the visual aids such as layout, design consistency, or graphical clarity. This could enhance overall engagement and make the presentation more visually appealing • The team could have used visuals in their presentation like charts, tables, etc.

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	125	250	0	0	0	125

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
1445	442

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	25	25	25	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
38697.99	86.00%

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
1176

Green Team Survey Comments
• Great job! • sysadmin admin user • Site crashed before I could try the admin account. • Does not load website • Did not load and gave a time out error. • Unable to load. • website will not load • Great job, good luck! • "Slight variations #1 sysadmin sysadmin@enegy.com Admin Demote Delete --- there is a backdoor or maybe unauthorized account #2 main page --- the template indicates the water should be viewable underneath the footer, the image is not a perfect match HOWEVER the criteria for marking true are present." • extra admin • Site is down