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

VIRGINIA TECH

PWN@VT

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 31 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	720	48.00%	9
Security Documentation	909	72.72%	71
C-Suite Panel	1024	81.92%	42
Red Team	750	30.00%	53
Blue Team	1724	86.20%	48
Green Team Surveys	1325	88.33%	50
Deductions	150		
Overall	**6302**	**63.02%**	**50**

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	720

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	Yes
6	Yes	11.3	Yes	22	
7		11.4		23	
8		11.5		24	
9	No	11.6		25	No
10.1	Yes	11.7		26	
10.2	Yes	12	No	27.1	Yes
10.3	Yes	13		27.2	Yes
10.4	Yes	14		28	Yes
10.5	Yes	15	Yes	29	No
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	909

Strong Points	*Areas of Improvement*
• system hardening was formatted and structured in a way that was very easy to follow • The team's system hardening strategies were extremely well done. They were easy to understand and their objectives were clearly addressed. • The hardening steps were documented well. • In the system hardening "System integrity and usability were prioritized over purely aggressive lockdowns." This is a novel idea that was not deployed by many teams, but will read well to the c-suite. Great job here.	• Network diagram is landscape, rather than portrait. Assume most people these days use PDFs and do not want to rotate manually. Network diagram also did not link connections between systems. • The system overview section would benefit from more specific information on the function of each asset. • Several key vulnerabilities were not documented. • The system overview was missing key components, and it should not have focused so much on the scenario itself.

Strong Points	Areas of Improvement
The organization in the system hardening section was well done, it would be even better if you explained why you took this path of organization. • System hardening and justification.	• HMI second service not listed. List host name in network diagram. More vulnerabilities should have been listed, missing unsecured user accounts. Make sure acronyms are spelled out before being used (e.g., DoS). • Analytical skills could be stronger, particularly when it comes to data interpretation.

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	1024

Strong Points	Areas of Improvement
• Good suggestions for priority recommendations and having everyone help present together. • I thought the Risk Reduction Strategy and Risk Matrix was strong & Recommendations Roadmap • I like the risk reduction strategy layout, easy for me to follow. Supply Chain Security, I love the recommendation, the 50k price tag could hold it back. When its a tough cost to estimate, you could consider different delivery. i.e. Work with our contracts dept to implement cybersecurity requirements for all contracting actions, this would include x, y, z. Unless I know the org cant implement this with current staff or a specific investment in software / hardware, I want to keep their focus and support on the idea. • Didn't get too far into attributing the event, just acknowledged the timing re: contractor access during maintenance. • The information was well presented and the slides were professional. • The team clearly defined each member's role, and every participant had meaningful screen time, which added to the professionalism and balance of the presentation. The visual aids were excellent, and each presenter delivered their section confidently and effectively	• Business risk should include how much money is at risk to be lost. Strategy was related to the incident and not correlated to mitigating business and operational risks. Unclear what individual contributions were. Some slides hard to read • Include total projected loss in revenue and how much the organization makes per day in revenue to see the impact of the breach. How does it affect the Public Relations image of the organization? • Would have liked to see some no cost recommendations. • A recovery roadmap isn't the same as a risk-reduction strategy. Didn't tie risks back to the bottom line • The high priority recommendations were costly, and lower cost/free options should be further explored. • This was a well-executed presentation overall. Continue refining your professional delivery and maintaining that strong team coordination as you move toward real-world scenarios.

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
125	125	0	0	125	0	125

Whack a Mole		
WAM1	WAM2	WAM3
125	125	0

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	249

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
21795.60	48.43%

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
1325

Green Team Survey Comments
• homepage footer • Wrong accent color • Footer is not available on the home page • no homepage footer • Could not scroll on the main page to verify the footer text, also the color was a little more red. Good luck! • Accent color appears more red than burgundy, but looking at the range of burgundy, it looks like some would consider this within the range. Nice work • footer doesn't stay at the bottom of the screen. • guys please make the footer right on the homepage • homepage footer • "This site cant be reachedweb.blue0031.cfc.local refused to connect. Try: Checking the connection Checking the proxy and the firewall ERR_CONNECTION_REFUSED" • Site is down