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

DEFENDING U.S. ENERGY INFRASTRUCTURE

TEXAS A&M UNIVERSITY

RET2REV

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 71 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	718	47.87%	10
Security Documentation	976	78.08%	64
C-Suite Panel	903	72.24%	75
Red Team	1375	55.00%	22
Blue Team	1975	98.75%	3
Green Team Surveys	1390	92.67%	20
Deductions	0		
Overall	**7337**	**73.37%**	**20**

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	718

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

1	Yes
2	
3	
4	Yes
5	Yes
6	
7	
8	
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	
11.1	Yes
11.2	Yes
11.3	Yes
11.4	Yes
11.5	Yes
11.6	
11.7	
12	No
13	
14	
15	Yes
16	Yes
17	Yes
18	Yes
19	Yes
20	Yes
21	
22	Yes
23	Yes
24	Yes
25	
26	
27.1	Yes
27.2	Yes
28	No
29	No
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	976

Strong Points	*Areas of Improvement*
• The team’s report includes a clear and useful diagram that helps visualize the environment. Their Active Directory and Linux findings are well analyzed, and mitigations are reasonable. The sections are logically structured and easy to follow. • This team's submission was rated as proficient in three key areas: the System Overview, Asset Inventory, and Network Diagram. The overview clearly explained the business purpose, the inventory covered most (70%+) of the required details, and the diagram provided good situational	• A few vulnerability entries mention SMB and FTP exposure under the database server, even though these services are not listed in the asset table; these should be verified and corrected. • Adding a legend and system labels to the network diagram would make it easier to interpret. • Each hardening step should include a short explanation of its purpose, and a brief summary of the top risks would make the report more concise and actionable.

Strong Points	*Areas of Improvement*
awareness. Additionally, their hardening approach was noted as technically sound and appropriate, using credible, open-source tools like PingCastle and Lynis. • The vulnerability and hardening sections are detailed, practical, and demonstrate a well-planned security approach across multiple systems. • The asset inventory and a good majority of the vulnerabilities were identified and resolved. • The team did a great job of defining and investigating the vulnerabilities and mitigations.	• To achieve technical accuracy and rule compliance, the team must replace prohibited port-blocking controls with allowed methods (like hardening and ACLs), complete all vague vulnerability mitigations by specifying exact control parameters, and bring the asset inventory to the "90%+" standard by adding all required services (notably SNMP on the DB). For presentation and audience, the system overview must be rewritten for senior leadership by moving technical details out, the network diagram must be elevated to "exemplary" by adding a legend and logical data flows, and the entire document needs a professional polish to fix typos and ensure perfect consistency. • Adding a concise summary or diagram at the start would make it even easier for leadership to quickly understand the overall security posture. • There is hardly any proper justification for why the system hardening steps were taken. • The System Overview is very brief and could be developed more, as is the Asset Inventory. While the network diagram does a great job of displaying the VPN and Cloud connections, it doesn't show the logical connections between components within the network. The System Hardening section should be more descriptive of tools and policies used and more clearly define each recommendation to senior management, it is currently very brief.

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	903

Strong Points	*Areas of Improvement*
• Excellent confidence by presenters. Covered the risks and plan well. • Good work on specifying the team roles. • Sound is too low, recommend moving closer to the camera/microphone. • Overview makes it sound like the malware was intentional by the third party employee.	• Zoom in with camera to both speakers and screen. Screen font too small to read based on camera zoom. Adjust camera position to minimize screen glare. Speakers are too soft due to distance from camera/mic. Too long - 6:34. Did not see any discussion of financial impacts of issue or remedy costs.

Strong Points	*Areas of Improvement*
If so this would be a criminal manner and law enforcement would need to be contacted. • Overview has jargon may be unfamiliar to C-Suite. • Business Risks - financial loss risk should be explained. How was this value calculated. • Strategies, include discuss of staffing, software, hardware, cost and timelines, staff training requirements, etc. • Training discussed, should include discussion of costs, timeline, and who conducts the training. • Reference list should be included with list of items reference such as NIST. • Good job articulating the risks, instead of just talking about the incident. Good job with high priority actions; you tied them back to ICS risks, but make sure to avoid jargon. • Presentation appeared professional but was difficult to see (no points deducted). • The high priority actions mostly were clear, immediate actions that would reduce risk.	A visual timeline showing your recommendations would have been very helpful. Inability to see/read slides really distracted from the presentation. • As an assessment team we want to frame the situation with facts and neutral tone. It sounds as if you are accusing the vendor of doing this on purpose, be sure to have the evidence to support this claim. The distinction between intentional acts and negligence is important. It affects legal liability, relations, and the credibility of your team and the organization. You are briefing the C-suite because what you say matters; they consider you experts and trust your assessments. • Font size is too small to read camera should be closer to the screen, or font should be larger. • Good work reference NIST guidelines • Only one of your strategies was thinking long term, and it wasn't clear how they would reduce the risks you had just talked about. I was not able to see the slides, and you should be within 15-20 seconds of the 5 minute mark. • Presentation was exceeded the target time. Strategy should be better defined and more directly related to the presented risks. • I was unable to read your slides at all. That would be very frustrating and distracting for the C-Suite.

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	0	125	250	0	125

Whack a Mole		
WAM1	WAM2	WAM3
250	125	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
1460	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	27	27	22	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
49567.33	110.15%

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
1390

Green Team Survey Comments
• The footer is not attached to the bottom of the page on the home screen • The footer is not on the bottom of the webpage • Excellent work!

Green Team Survey Comments
• Admin button is present when you login as user (Admin Middleware). • Everything working as expected. Good job! • Good job • The tagline is at the top of the image rather than the center of the image of the website. Your rig is in 'Normal Operation'. • 5:48 This site can’t be reached