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

THE PENNSYLVANIA STATE UNIVERSITY

CYBERLIONS-B

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 14 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	315	21.00%	73
Security Documentation	1191	95.28%	13
C-Suite Panel	1085	86.80%	25
Red Team	2000	80.00%	4
Blue Team	1675	83.75%	54
Green Team Surveys	1123	74.87%	16
Deductions	0		
Overall	**7389**	**73.89%**	**16**

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	315

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

1	No
2	
3	
4	
5	
6	
7	No
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	No
11.1	Yes
11.2	Yes
11.3	Yes
11.4	Yes
11.5	Yes
11.6	Yes
11.7	Yes
12	
13	
14	
15	Yes
16	No

17	Yes
18	Yes
19	No
20	Yes
21	
22	No
23	
24	No
25	No
26	
27.1	Yes
27.2	Yes
28	No
29	No
30	

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	1191

Strong Points	*Areas of Improvement*
• Strong justifications were provided for the system hardening steps. An extensive list of vulnerabilities was provided. • The team's mitigation strategies were very well thought out. • This document stands out for its depth and accuracy. • The team demonstrated a strong understanding of both Windows and Linux hardening and provided clear, actionable mitigations. • The report's structure is polished, logical, and communicates technical information in	• The system overview was well written but lacked an focused discussion of the system's purpose. • The network diagram was inconsistent with the provided asset overview. Some key vulnerabilities were not reported. • The IP address for the AD/DNS server in the asset table should end in .141, not .145, to prevent confusion with the Web server. Some vulnerabilities appear under the wrong host due to this mismatch and should be corrected.

Strong Points	*Areas of Improvement*
a way that decision-makers can easily understand. - Covered great amount of details with clarity and looking good to present. Great effort, too many good details in all the sections. - The overview document was senior leadership appropriate	- A short one-page summary highlighting top vulnerabilities and risks would be helpful for leadership review. - Overview of the system to impress the executives with clear non-technical language can help. - Identifying only actual vulnerabilities as opposed to perceived

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	1085

Strong Points	*Areas of Improvement*
- The background of the incident was great and the ability to understand and focus on containment first is critical. The team seemed cohesive with their presentation and was done well with the transitions. A leadership team appreciates the clear view that the slides present. - The thoughts and ideas were well thought out and explained well. - Strong link between operational disruption, safety, and business credibility. Presentation shows good integration of cost-effective mitigations. - Risk was clearly defined and explained. Good work on presenting the slides. Students identifies themselves or the next presenter and their role. - All presenters were professionally dressed, the video image didn't get in the way of reading the slides, everyone one on the team presented a portion, the presenters spoke to the slides and didn't read them, and timelines and costs were given. -- Very well done! - Good job with immediate action plan. - Clean and professional presentation materials.	- The action plans are great and easy to understand but not sure that a lot of research was put into the timing and cost to implement. Segmentation of OT networks can take over a year depending on the size of the environment. Focus on slowing down when presenting. It was rushed and made it seem like you were on a timeline which is not the point of the presentation. And what is it that you would like as an action to come out of the meeting? Be sure to summarize the presentation with the action you need to come out of the meeting. - The slides were well done. There was one slide where the talking points were not in the same order as the bullets on the slide, which can cause some confusion and can be distracting. - Lacks depth in how actions mitigate specific risks. Narrative flow is a bit disjointed between speakers. - For the action plans, discuss if additional staffing or consultants will be hired for these tasks. This is quite a bit of work to add to the workload of the current staff of the organization. The timelines listed are very fast. It may take longer for actual implementation with testing, schedule downtimes, etc. - Recommend final slide with references, and more details on specific software and hardware recommendations.

Strong Points	*Areas of Improvement*
	• Long-term strategy lists many bullets but doesn't go into much detail on the bullets, I recommend a tighter focus with a little more depth. • The only thing that could have improved this is if there had been some graphics added to the slides. • Impact is only one factor in risk. What is the likelihood of each cyber threat? • You specified risks. How does your immediate risk reduction strategy reduce those risks? • When estimating costs, remember that labor is NOT FREE, even if it is done in house. Every hour your cyber or IT team is spending on configuring/using network monitoring tools is an hour not spent on something else. • The strategy to reduce the identified risk of potential injury wasn't clear.

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	250	125	250	250

Whack a Mole		
WAM1	WAM2	WAM3
250	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
1460	215

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)
24	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
18862.93	41.92%

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
1123

Green Team Survey Comments
• login for users not working. website down after attempting to log in. • Website went down halfway through survey • The site failed while I was viewing it. When I logged into the green-user account, it went to an internal server error. ErrorException: Undefined variable $active • Website does not load. • "Internal Server Error Undefined variable $active" • site got hacked as I was going through survey • Site partially broken, very little to anything except for the Homepage and the 'Admin Dashboard' login screen. • Opps, red user got added. • Site is down