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

THE PENNSYLVANIA STATE UNIVERSITY

CYBERLIONS A

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 30 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	857	57.13%	4
Security Documentation	1200	96.00%	12
C-Suite Panel	1058	84.64%	31
Red Team	1750	70.00%	8
Blue Team	1945	97.25%	11
Green Team Surveys	1369	91.27%	5
Deductions	0		
Overall	**8179**	**81.79%**	**5**

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	857

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	No	10.9	Yes	19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	Yes
6	Yes	11.3	Yes	22	Yes
7	Yes	11.4		23	No
8		11.5	Yes	24	No
9		11.6		25	Yes
10.1	Yes	11.7		26	No
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	Yes
10.6	Yes	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	1200

Strong Points	*Areas of Improvement*
• Well written systems hardening section. Great job! • Correct technical terminology, clear formatting, and no major spelling/grammar errors. • Consistent template and clean presentation. • Documentation was detailed. • Your hardening techniques were very thorough and clearly reflected real technical understanding. The depth you provided shows strong potential for professional-level	• The system overview could be improved by providing context for the acronyms (DB, AD, and DNS) to better resonate with the targeted audience. Additionally, some areas lack detail regarding system definitions and purposes. • Break up dense text/tables for improved readability. • Use more section headings and visual breaks for clarity. • More detail could have gone into the system overview.

Strong Points	Areas of Improvement
documentation and defensive operations work. • I liked how you justified your mitigations for vulnerabilities in the Known Vulnerabilities section. The System Hardening section was also well-written; you all concisely explained what you did, how you did it, and why you did it. Love it!	• You're already producing strong, technically solid work. One small refinement that would take your presentation even further is adjusting a bit of the language for a C-suite audience. You clearly understand the material lightly reducing some of the technical jargon and tying a few points back to business impact will make your message even stronger. You're very close, a little polish here will elevate an already great effort. • Be consistent with your hostnames (e.g. Task Box).

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	1058

Strong Points	Areas of Improvement
• Great use of visual aids with appropriate amount of detail per slide • The presentation slides were nicely done. • Good breakout of the risks, very easy to follow. • I liked that the team put together clear costs for the proposed recommendations as well as detailed timelines that range from short term to long term (from 1 week of effort up to a year) • Comprehensive Risk Analysis (30% Weight): Team 30 provided a clear summary of both operational and business risks. The presentation effectively separated these concerns: • Operational Risks: Identifying direct consequences such as mechanical failures resulting in loss of the asset, impacts on employee health and safety (injury/death), and the resulting inability to provide oil and gas to customers. • Business Risks: Clearly translating operational failures into financial impacts, including loss of profit, potential regulatory violations (e.g., OSHA), and failure to meet service level agreements. The distinction was clear, non-jargon, and suitable for all members of the C-Suite.	• Strategy connection to operational and business risks could be more closely tied together. Costs of recommendations is unclear whether for licensing, labor, or other. • Strategy to reduce risk somewhat tied back to business risk, but the last two points were glossed over. The strategies and recommendations didn't really tie back to what the C-suit wants to hear, which is return on investment, especially on the recommendations that require additional funding. • I do like that the team put together clear costs for the proposed recommendations as well as detailed timelines that range from short term to long term (from 1 week of effort up to a year). The team is dressed appropriately and there are no visual distractions. However the slides could be put together for consistent formatting for a more professional look. Additionally the summary slide missed some key parts of the presentation • The risks are summarized within the context of the scenario but what his repeatedly hit upon is ""financial losses"". As an executive, I would want to know what precisely those

Strong Points	*Areas of Improvement*
• Complete and Coherent Strategy (30% Weight): The team presented a complete strategy to reduce risk. The strategy included three or more long-term action items/policy updates, such as establishing situational awareness, ensuring resilient infrastructure (backups), implementing employee training, and following the Department of Energy's risk management process. • Professionalism and Teamwork (10% Combined Weight): The presentation utilized slides and followed a professional, consistent structure, beginning with a clear agenda. More than two team members participated equally (McGuire, Aiden, Owen, Asa, Glenn, Hayden). The team ensured clear acknowledgment of contributions as speakers transitioned, meeting the highest criteria for presentation elements • Good work having each student introduce themselves by name and job role. • Professional presentation with content and videos embedded. • Nice slide design and graphics. • Well designed slides. Nice transitions. Good color scheme. Good professional headshots of presenters.	losses would be, even if the dollar value is a guesstimate. Executives know there will be a financial impact in any scenario, what they need to know is the order of magnitude of that impact, simply saying there will be losses without quantifying them isn't enough information to make decisions. • The team does provide a reasonable strategy to reduce risks that are related to the identified issues however the strategy does not clearly address all previously identified risks. For a risk reduction strategy, the team recommends having situational awareness. How do you propose that take place? Would it be through network traffic monitoring? End point detection monitoring? A SIEM? • The video is the appropriate length per the guidelines however it is too short for the amount of information provided. For example, the team recommends using DOE's Risk Management Process but doesn't say why that is a recommendation to reduce an identified risk, just that it is. In a real world scenario, there would be time for Q&A to ask questions like that but given this exercise, I think it would have been best to simply stick with risk reduction strategies 1 through 3 because as there was some reason provided as to why they are being recommended and the team could still stay within the video length guidelines for the project. • The high priority recommendations are well thought out, clearly communicated, and reasonable for the real world. However this scenario demands that actions require minimal levels of additional funding and highlights the use of free or open-source tools. None of the recommendations are low to no cost. But because they are presented and justified well, this would be acceptable to a C-suite exec, just expect some negotiations to take place ;). • Adherence to Funding Constraints for Recommendations (30% Weight): The C-Suite briefing emphasized that current funding is extremely limited (or non-existent) and that high-priority actions should use free or open-source tools. The Exemplary

Strong Points	*Areas of Improvement*
	criteria require actions to demand ""at most a minimal level of additional funding"" • To Improve: Focus should be placed on high return-on-investment actions that require minimal or zero additional funding, such as simple policy updates, immediate fixes (like patching or closing unnecessary ports), or planning/tabletop exercises, especially when using open-source tools. While costs were justified by providing the expected cost, timeline, and benefits, the magnitude of these costs contradicted the stated constraint of ""minimal funding"" • Key risks should also be quantified for financial losses, and downtime, etc. • Risk reduction discussion needs further details, for example what is the recommendation to enhance situational awareness. • Short-term action items should be explained at a level for non-IT professional C-Suite members. • It is unclear how the cost of staff related to the SIEM was determined. • The organization is currently breached, hiring penetration testers at this time may be premature and could be moved to long term goals after the current break is remediated. Penetration test. • The Agenda and Summary slides could be removed and additional time could be used to add further details and context to the slides. • Audio seems to be altered to go at a faster speed. If not the speakers are speaking at a very fast speed. Rate of talking was too fast to comprehend on a single viewing. • For strategies associated staffing costs should also be discussed. • For references, recommend including the name of the article in addition to the url. • Risk should be quantified, financially. • The organization likely has anti-virus, other solutions such as network segmentation could explored.

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	125	250	125	125	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
1475	470

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
41068.50	91.26%

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
1369

Green Team Survey Comments
• Everything's here and it looks great! Clean, easy to use, and really well put together. • Excellent work! • Looking good • Great job! You secured that oil rig so tight even the crude couldn't slip past you! • Nicely done! • all good • web.blue0030.cfc.local took too long to respond. • Site is down