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

OREGON STATE UNIVERSITY

WICYS OSU

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 96 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	321	21.40%	71
Security Documentation	1078	86.24%	43
C-Suite Panel	1029	82.32%	39
Red Team	875	35.00%	44
Blue Team	1428	71.40%	77
Green Team Surveys	1375	91.67%	56
Deductions	0		
Overall	**6106**	**61.06%**	**56**

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	321

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		10.9	No	19	Yes
4		11.1	Yes	20	No
5	Yes	11.2	Yes	21	
6	No	11.3	Yes	22	
7	No	11.4		23	
8		11.5		24	No
9	No	11.6		25	
10.1	Yes	11.7		26	
10.2	Yes	12		27.1	Yes
10.3	Yes	13		27.2	Yes
10.4	Yes	14		28	No
10.5	Yes	15	Yes	29	
10.6	No	16	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	1078

Strong Points	*Areas of Improvement*
• Excellent inventory & system diagram. • The network diagram is well done and includes the logical connections to different systems on the network, in addition to a legend which helps with readability. It is an interesting choice to include the "unauthorized node" that is assumed to be a breach. That's not an asset that the company owns, so it's not considered part of normal operations for the site. • Vulnerabilities and their mitigation are comprehensive with strong technical reasoning.	• System Overview - remember when your English teacher said to avoid one big paragraph - it's true. Missing vulnerability listing for HMI & PLC. No hardening plan for HMI & PLC VMs. • The Vulnerabilities and Mitigations list and the System Hardening sections do not include HMI and PLC systems. This should be reviewed and those systems included, otherwise there are vulnerabilities that will persist for the site. Also the System Hardening has good information for the 4 systems it does include, but the

Strong Points	Areas of Improvement
• The vulnerability and hardening sections show impressive attention to detail and strong understanding of how to secure a complex environment. • Overall good documentation, and the network diagram appears to have a lot of work put into it.	organization of the information and the professional presentation when it comes to formatting could be improved. For example, each section in System Hardening could have the description and recommendations detailed first and then list the tools used afterwards. and possibly consider using simple table for each section. • Break up dense tables and long paragraphs into shorter, easier-to-read sections. Add more subheadings and visual breaks as needed. • Some sections could be shortened or summarized more for leadership readers to make the document quicker to review. • The system hardening should focus on the overall system in general and not specific items for each machine.

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	1029

Strong Points	Areas of Improvement
• The team set a high standard for presenting information in a clear, legible, concise, and impactful manner. They touch on key topics such as financial impacts, business continuity. The recommendations and their impacts are clearly laid out with important financial expenditures, and justifications, provided for each recommendation. The high priority recommendations and the strategy are interwoven making it hard to determine which is which from a grading standpoint but the manner in which everything is tied together tells a powerful story that would resonate with C-suite executives. • Identification of risks relevant to business concerns were solid, especially in alignment with some of the high-priority recommendations. Good job about being mindful of costs and advocating for recommendations aligned the incident presented. Big props to bring up third-party/vendor management.	• My only recommendation would be not to have sped the video up so drastically. It was a clever way to reach the 5 minute presentation limit but could make it difficult for others to follow. • The presentation attempts to squeeze a lot of details into the five minute time period. The fast cadence of the presentation and jumps in the audio makes it a bit jarring / hard to follow at times. For example, the speed makes recommendations about software end up being a bit confusing (ex: estimated cost for Anti-Virus being presented as 0$, $200-300 and then listing different products as choices - it may be better to stick with a low-cost option for brevity and the specific FOSS requirements in the presentation ask) • Certain details regarding the incident overview are a bit too 'in-the-weeds' technical and may not be needed as that would provide more time to focus on risks and strategy. There is blurred-line between

Strong Points	*Areas of Improvement*
• Good variety of products suggested for each solution. • This information was great and presented professionally • Well designed slides • Professional visuals and presentation. One of the more polished slide decks.	strategy and high-priority recommendations, it would likely be beneficial to present the strategy at a higher level to give C-Suite a solid direction to move the organization in instead of individual tactical implementations. • Speeding up the recording made it hard to follow. It wasn't clear which items were risk-reduction strategies, and which were high-priority recommendations. Neither was clearly tied back to the risks. • Some of the slides were a little busy and had a little too much information. Consider more slides in the future. • Should state the roles or work completed of the team members • Speaking speed seems adjust to run faster. Makes it very difficult to comprehend. If the speakers ran overtime the video should have been edited or reshot. • Loss should be quantified financially • Strategies should include example software, hardware, training, etc.. • Jargon should be minimized as the C-Suite may not be IT experts • The institution probably already has anti-virus. This should be updated with a more relevant recommendation. • Conclusion could include list of recommendations such as software and hardware. • For references include name of article • The presentation like an audiobook at 2x speed. It was hard to keep up - might be information overload for many executives.

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	0	250	0	0	0

Whack a Mole		
WAM1	WAM2	WAM3
250	0	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
1410	18

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)
22	22	24	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
1600.64	3.56%

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
1375

Green Team Survey Comments
• green user got deleted • Recommend you check your menu that appears when you change resolution/minimize screen, at full screen Admin button is hidden from a normal user but when minimize and scale the

Green Team Survey Comments
screen down and the collapse menu appears Admin appears when menu expands, don't believe this was an attack just thinking missed in coding - suggest fix as others may operate in that resolution and mark the test fail. • The site is slightly lighter than the rest. It is still maroon but it is bordering orange to me. No admin button when logged in or user management. • site color is red/pink • The site color was more red and not the maroon/burgundy. Good luck! • The color is a bit suspicious. • green user missing from user management, color too light • This site can't be reachedweb.blue0096.cfc.local refused to connect.