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

OREGON STATE UNIVERSITY

OSUSEC

November 9, 2024

In-Person

Number of Teams	Max Team Points Received	Min Team Points Received	Mean Team Points Received	Total Points Possible
94	9153	1350	6115.31	10,000

TEAM 64 SCORECARD

This table highlights the *team's* efforts for the 2024 CyberForce Competition®.

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	1015	50.75%	11
Security Documentation	909	90.90%	26
C-Suite Panel	868	86.80%	37
Red Team	1900	76.00%	11
Blue Team	1990	99.50%	32
Green Team Surveys	1132	75.47%	11
Deductions	0		
Overall	**7814**	**78.14%**	**11**

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. Most anomalies are mapped to the NIST NICE Framework and fall into one of seven work role categories: *Oversight & Governance, Design & Development, Implementation & Operation, Protection & Defense, Investigation, Cyberspace Intelligence, and Cyberspace Effects. Some anomalies may also be categorized as Energy or "Other".* For those mapped to the NIST NICE Framework, their will include the mapping to associated knowledge, skill, ability, and task roles within its respective category, offering students with a comprehensive idea of the wide range of responsibilities cybersecurity professionals face while in the field.

Anomaly Score	1015

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

1	yes	27	no	53	yes
2	no	28	yes	54	Not Answered
3	yes	29	no	55	yes
4	yes	30	no	56	no
5	yes	31	no	57	yes
6	yes	32	Not Answered	58	yes
7	yes	33	Not Answered	59	yes
8	yes	34	yes	60	no
9	yes	35	Not Answered	61	yes
10	yes	36	yes	62	yes
11	yes	37	no	63	yes
12	Not Answered	38	yes	64	no
13	yes	39	yes	65	yes
14	yes	40	yes	66	yes
15	no	41	yes	67	yes
16	yes	42	Not Answered	68	yes
17	yes	43	Not Answered	69	Not Answered
18	yes	44	yes	70	yes
19	no	45	yes	71	no
20	Not Answered	46	yes	72	yes
21	yes	47	no	73	Not Answered
22	Not Answered	48	yes	74	no
23	yes	49	yes	75	Not Answered
24	yes	50	yes	76	yes
25	Not Answered	51	yes	77	yes
26	Not Answered	52	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 overview relates to business functions and addresses senior leadership well. • This submission had a lot of strong elements - system overview, network diagram, asset inventory, vulnerabilities, and system hardening. One detail that I want to emphasize is the details addressed in the professionalism and formatting of the report. By using varied font characteristics and/or formatting, the messages communicated by the team would be efficiently, and effectively received by senior management. This is an example of a small, but impactful attribute. • The documentation of asset inventory, vulnerabilities, and identified mitigations was clear and well-written. • Amazing overview, very detailed. Great network diagram. • Thorough descriptions on hardening steps. Easy to understand explanations, well formatted. • This entry showcases an excellent understanding of system security and hardening practices across a diverse set of operating systems and machines. It effectively highlights specific actions taken on each system, such as removing backdoors, updating software, enforcing password policies, and configuring firewalls. The level of detail reflects strong planning and prioritization, with a clear focus on both preventive and detective security measures key strengths in any security assessment. •	• Because the network diagram is intended to help new staff respond to incidents, asset-specific IP information should be provided. • Possibly consider adding a legend to the network diagram. It was not a fault because each asset was labeled, but a consolidated legend is still a recommended best practice. • The network diagram needs improvement to convey information effectively. It should include clear representations of logical connections. Ensuring technical accuracy and using standard symbols is crucial. • Nothing to note. • While the entry is already detailed and thorough, it could be even stronger by adding a more structured summary of the overall security improvements and remaining risks. A high-level overview or risk assessment at the end would provide a clearer picture of the system's security posture following the hardening efforts.

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	868

Strong Points	*Areas of Improvement*
• I like the explanation of "what happened," it made for a clear flow throughout the presentation. I also appreciated the very specific impacts and business financial risks. • The split between presenters was well done and made a clear delineation in topic being covered. The further explanation of slides was helpful as well. • Good research on the specific impacts to wind power industry • The team effectively identified key business risks resulting from the cyberattack, including reputational, operational, and financial threats. Their risk mitigation strategies were practical and actionable, covering critical areas like training staff on security fundamentals, implementing strong login methods, and maintaining an asset inventory. Additionally, the emphasis on endpoint detection and a Security Information and Event Management (SIEM) system demonstrated a proactive approach to protecting the organization's infrastructure. The entry also clearly highlighted the potential impact on national infrastructure, reinforcing the importance of maintaining compliance and service reliability.	• The first presenter talked a bit too quickly, making the beginning difficult to follow. Additionally, it was implied that the high priority actions were free and open-source, but this was not clearly stated. It is important to highlight the bottom line for the C-suite. • Reduce word count on slides and verbally expand on the areas. Keep key topics as bullet points. Specific free and open source tools would be helpful to mention to give the C-Suite something to look into if they are interested in learning more about what is available. • Some strategies and priorities would only work on IT systems in the enterprise • The entry could be improved by enhancing its organization and clarity to strengthen the presentation's flow and accessibility. Outlining risk mitigation strategies alongside each identified risk would make it easier for the audience to follow the connections between threats and solutions. Adding specific examples or tools for each recommended action (e.g., naming open-source authentication options or SIEM tools) would also provide practical, implementable suggestions. Lastly, discussing how the organization will prioritize and phase the recommendations—especially if budget constraints exist—would help the C-Suite better understand the strategic roadmap and make informed decisions about immediate versus long-term actions.

RED TEAM SCORING

Red Team Flag Inputs (Assume Breach & Whack a Mole)

This year we will be using ***Assume Breach*** for part of your Red team score. This will be worth *1000 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	AB8	AB9	AB10
100	75	100	50	50	100	100	50	50	25

Whack a Mole	
WAM1	WAM2
375	375

AUTOMATED SCRIPT CHECK – VULNERABILITY

This portion of the Red team score will be worth *750 points*. This will be done via an automated scripted check.

Automated Script Score	450

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	AI Algorithm Score
1590	400

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
1132