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

UNIVERSITY OF TULSA

ROOT66TULSA

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 75 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	652	32.60%	45
Security Documentation	854	85.40%	44
C-Suite Panel	855	85.50%	41
Red Team	1038	41.52%	60
Blue Team	1472	73.60%	82
Green Team Surveys	521	34.73%	65
Deductions	0		
Overall	**5392**	**53.92%**	**65**

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	652

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

1	yes	27	no	53	no
2	no	28	Not Answered	54	no
3	yes	29	Not Answered	55	yes
4	yes	30	Not Answered	56	no
5	yes	31	Not Answered	57	yes
6	yes	32	Not Answered	58	yes
7	yes	33	no	59	yes
8	yes	34	no	60	no
9	yes	35	Not Answered	61	yes
10	yes	36	yes	62	yes
11	no	37	yes	63	yes
12	yes	38	Not Answered	64	no
13	yes	39	Not Answered	65	Not Answered
14	yes	40	yes	66	Not Answered
15	no	41	Not Answered	67	Not Answered
16	yes	42	no	68	Not Answered
17	yes	43	yes	69	Not Answered
18	yes	44	Not Answered	70	Not Answered
19	yes	45	no	71	Not Answered
20	yes	46	yes	72	Not Answered
21	yes	47	no	73	Not Answered
22	no	48	yes	74	Not Answered
23	Not Answered	49	yes	75	Not Answered
24	no	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	854

Strong Points	*Areas of Improvement*
• Outstanding Network Diagram, Asset Inventory, and Vulnerability list. • This was a well-balanced document. • The section on known vulnerabilities is well done. Great job! • Their document is technically sound and concise.	• The System Hardening and Document format required just a bit more polishing. Regardless, fantastic job! • I few more details on all sections would have made each category perfect. • The section on system hardening could benefit from further elaboration on the specific steps involved. Providing a detailed breakdown along with justifications for each action would enhance the clarity and effectiveness of this section. • By adding missing required asset and services in "Asset Inventory", and improving formatting.

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	855

Strong Points	*Areas of Improvement*
• Well done! The high-priority action items in the presentation are well thought out, providing a comprehensive set of actions. • Good work identifying risks to OT systems as well. Slides were well designed. Easy to read, and I liked the use of the associated clip art/graphics. Good work on including url references on slides so that viewers can follow up on these points. • The risks were directly tied to financial loss, which is exactly what the C-Suite needs to be informed about. • The presentation had a strong introduction that contributed to the continuity of the presentation. • Good understanding and understanding of the risks and consequences to the business and clearly communicated.	• Great start! There's an opportunity to improve by condensing the information, which could help maintain a steady and engaging pace throughout the presentation. • Recommend including the team members names on the first slides. Video is 7 minutes and 19 seconds long. This is over the recommendation of 5 minutes. There is discussion of removal of infected systems. Clarification is needed as to why these systems cannot be remediated instead of being replaced. Regarding the recommendation to transfer IT staff temporarily to Cybersecurity. Are these staff trained in Cybersecurity or will they need training. Is this leaving IT understaff causing further risks? Are tools paid or

• Good idea to have IRP, BCP and DR for risk reduction, they are crucial tools in today's cybersecurity landscape. •	open source needed for network mapping and vulnerability assessment? Costs and tools should be discussed. Monitoring and logging is stated as no additional costs. Recommend discussing tools and associated costs, or open source for clarity. Discussion of who is conducting the security awareness training and how is it funded? • Your presentation was 7 minutes long. Parts of the presentation could have been eliminated, such as the summary. • Attempting to explain technical strategy to the C-Suite is unnecessary. Simply state how the strategy will reduce risk. • For the priorities, you mention "labor hours". Expand on that cost, as well as the return on investment of those labor hours. Spend less time listing all the departments in the business, simply state "all department leaders". • The graphics in the lower right hand corner of the slides could have been distracting from the otherwise excellent slides. •

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
0	50	50	100	0	75	0	50	25	50

Whack a Mole	
WAM1	WAM2
93	93

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
1400	72

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
521