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

UNIVERSITY OF ILLINOIS CHICAGO

0X1BADB002

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 2 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	996	49.80%	13
Security Documentation	913	91.30%	24
C-Suite Panel	783	78.30%	63
Red Team	1613	64.52%	25
Blue Team	1990	99.50%	32
Green Team Surveys	1279	85.27%	16
Deductions	0		
Overall	**7574**	**75.74%**	**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. 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	996

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

1	yes	27	no	53	no
2	no	28	no	54	yes
3	yes	29	no	55	yes
4	yes	30	Not Answered	56	no
5	yes	31	no	57	yes
6	yes	32	yes	58	yes
7	yes	33	yes	59	yes
8	yes	34	Not Answered	60	no
9	no	35	Not Answered	61	no
10	yes	36	yes	62	yes
11	no	37	no	63	yes
12	yes	38	Not Answered	64	no
13	Not Answered	39	yes	65	Not Answered
14	yes	40	yes	66	yes
15	no	41	yes	67	yes
16	yes	42	Not Answered	68	yes
17	yes	43	no	69	Not Answered
18	yes	44	no	70	yes
19	yes	45	yes	71	no
20	yes	46	yes	72	no
21	yes	47	no	73	Not Answered
22	yes	48	no	74	no
23	Not Answered	49	yes	75	yes
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	913

Strong Points	*Areas of Improvement*
• Good work on network diagram, and asset inventory. • Thorough detail on asset inventory and vulnerabilities • Excellent document with fully developed system analysis. The hardening directly corresponded to discovered vulnerabilities. • Asset inventory very strong, documented all ports and highlighted required.	• Did not identify majority of vulnerabiities. • Found many but not most of the vulnerabilities • Hardening steps directly corresponded to discovered vulnerabilties. However, there are certainly other forms of popular, powerful tools which can be easily deployed for defense bolstering. • Some inconsistency with font and minor typos/formatting issues. • Known vulnerabilities were not organized and a server was missing.

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	783

Strong Points	*Areas of Improvement*
• Good summary of business risks. I appreciate the comparison of the cost of your recommendations versus the cost of not implementing them. • Focus of screen on slides is helpful for viewer. Presenters are well-spoken and dressed professionally. • The long-term strategies are very well explained and relate directly to the business risks. • One of the elements that stood out was how polished and professional the presentation looked. As well as the detailed summary of financial risks, especially the way it compared a potential budget to potential operational losses. It really showed a deep consideration of the financial aspects.	• What are your long term strategies, and why are you implementing them? Strengthening Cyber Security is a goal, not a strategy. • Reduce or remove reference to specific government entities (military, Department of State, etc.) as specific government agency using this energy company are not specified. Also, it is not denoted whether the government is their biggest contract so those references should be removed as well. The CFO could very likely latch on to those topics, and if they are false, the CFO will lose trust/faith in your ability to speak to cybersecurity. While this is unfair, it is typical in the workplace. Overall, great job! You both presented the information thoroughly and clearly. • The cost was far too high at $137,000/month.

	• I really appreciated the effort put into the presentation and thoroughness of content but it did exceed the 5 min. I noticed there were some instances where you were reading directly of the slides and a few 'umms'. Perhaps practicing a bit more could have help reduce dependency on slides. I was once told that by the time I finished reading the slides maybe some of the audience may have finished doing so which loses engagement. A few more images or bullet points could have been more engaging.

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	100	50	100	100	50	50	75	25	50

Whack a Mole	
WAM1	WAM2
375	187

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
1279