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

INDIANA INSTITUTE OF TECHNOLOGY

CYBER WARRIORS

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 22 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	432	21.60%	80
Security Documentation	727	72.70%	68
C-Suite Panel	678	67.80%	76
Red Team	1900	76.00%	11
Blue Team	1915	95.75%	50
Green Team Surveys	43	2.87%	58
Deductions	0		
Overall	**5695**	**56.95%**	**58**

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	432

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

1	yes
2	yes
3	yes
4	yes
5	yes
6	yes
7	yes
8	yes
9	yes
10	yes
11	no
12	Not Answered
13	yes
14	no
15	Not Answered
16	Not Answered
17	Not Answered
18	no
19	yes
20	Not Answered
21	yes
22	Not Answered
23	Not Answered
24	no
25	Not Answered
26	Not Answered
27	no
28	yes
29	Not Answered
30	Not Answered
31	Not Answered
32	Not Answered
33	Not Answered
34	Not Answered
35	Not Answered
36	yes
37	yes
38	Not Answered
39	yes
40	no
41	Not Answered
42	Not Answered
43	Not Answered
44	Not Answered
45	yes
46	Not Answered
47	Not Answered
48	Not Answered
49	Not Answered
50	Not Answered
51	Not Answered
52	Not Answered
53	no
54	Not Answered
55	yes
56	yes
57	yes
58	yes
59	yes
60	yes
61	yes
62	yes
63	no
64	no
65	Not Answered
66	yes
67	Not Answered
68	Not Answered
69	Not Answered
70	Not Answered
71	Not Answered
72	Not Answered
73	Not Answered
74	Not Answered
75	Not Answered
76	yes
77	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	727

Strong Points	*Areas of Improvement*
• Very complete asset list. • Good system overview. • The System Hardening section provided a comprehensive overview of the measures implemented and the tools utilized to enhance system security. • Their responses to "Asset Inventory" and "Network Diagram" were the best among all four sections because of their conciseness, and contained appropriate formatting.	• Good start on vulnerabilities, but needs more. Also, you need justifications for system hardening. • after reading your hardening steps there were vulnerabilities that you addressed that were not listed on the known vulnerability section. • I recommend creating a table to list the specific vulnerabilities identified for each system. It may be beneficial to include an IP address column to facilitate the mapping of these vulnerabilities. • By improving their response to "Known Vulnerabilities" and adding appropriate formatting to their response to "System Hardening".

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	678

Strong Points	*Areas of Improvement*
• Video editing and presentation • Good instructions given to C-Suite for resource allocation and mentioning C2M2 • This team covered all areas; listed clear summary of business and financial risks, provided strategy to reduce risks, recommended up to 3-4 high priority actions to improve overall security, appropriately dressed and video length and visual aids, slides and other materials have a consistent professional appearance • Good job identifying and communicating risks to the C-Suite!	• Instead of recommending as many actions as they did, further reasoning why the selected items are the most important and how they address the identified/given risks would be beneficial. • Heavy reliance on expensive commercial tools • This team did excellently well. The only additional recommendation would be to always explain technical terms in a business format such that a non technical person would grasp it. Your team did a good job explaining this but I would like to see a little more explanation for things like end point security, and back up recovery in the future. Overall good work and congratulations on a Job well done.

	• The quality and usage of slides was lacking. I think that increasing the number of slides would help. There were a ton of recommendations to implement but costs ranged from free to thousands of dollars. I think boiling these down to just a handful and having a single slide to communicate will help when talking to the C-Suite.

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
50	100	75	50	100	75	100	50	0	100

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
1515	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
43