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

PURDUE UNIVERSITY-MAIN CAMPUS

BLUE TEAM AT PURDUE

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 7 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	330	16.50%	86
Security Documentation	0	0.00%	88
C-Suite Panel	624	62.40%	84
Red Team	1013	40.52%	64
Blue Team	1608	80.40%	73
Green Team Surveys	301	20.07%	85
Deductions	0		
Overall	**3876**	**38.76%**	**85**

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	330

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

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

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	0

Strong Points	*Areas of Improvement*
•	•

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	624

Strong Points	*Areas of Improvement*
• Good selection of tools to improve security and explanations • great recommendations, they provided • The detailed information for each recommendation was well explained and slides were professional. • Good detailed priority recommendations (Voss/Nesus)	• Strategy could include more longer term solutions • Could you please clarify which recommendations specifically address the business risks and describe the mechanisms by which they accomplish this? The presentation currently relies on the audience to make these connections, and some may not possess the technical knowledge necessary to do so. • The video cut abruptly at the end and when one of the presenters was talking it was cut off abruptly as well just as he was about to finish. • Discuss greater financial cost to business

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	50	0	0	75	0	50	50	0	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
1540	68

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
301