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

DEPAUL UNIVERSITY

DEPAUL UNIVERSITY TEAM HEHE

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 50 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	546	27.30%	70
Security Documentation	0	0.00%	88
C-Suite Panel	588	58.80%	87
Red Team	1563	62.52%	30
Blue Team	1565	78.25%	75
Green Team Surveys	1298	86.53%	61
Deductions	0		
Overall	**5560**	**55.60%**	**61**

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	546

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	yes
13	yes
14	no
15	yes
16	yes
17	yes
18	yes
19	yes
20	no
21	yes
22	Not Answered
23	yes
24	yes
25	Not Answered
26	Not Answered
27	Not Answered
28	no
29	Not Answered
30	Not Answered
31	no
32	Not Answered
33	Not Answered
34	Not Answered
35	Not Answered
36	Not Answered
37	yes
38	yes
39	no
40	no
41	Not Answered
42	Not Answered
43	no
44	yes
45	Not Answered
46	Not Answered
47	Not Answered
48	Not Answered
49	Not Answered
50	Not Answered
51	Not Answered
52	Not Answered
53	Not Answered
54	Not Answered
55	yes
56	yes
57	yes
58	yes
59	yes
60	no
61	yes
62	yes
63	yes
64	yes
65	no
66	yes
67	Not Answered
68	yes
69	Not Answered
70	yes
71	no
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	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	588

Strong Points	*Areas of Improvement*
• Thorough overview of the strategy directly mapped to risks • The team effectively articulated the business concerns and associated risks. A specific point in the risks section provided a solid foundation for the subsequent security recommendations, and an introductory sentence helped to establish a clear connection between these two sections. • The risk to business reputation and the risk of litigation were mentioned. The strategy directly related to stated risks. • Strong explanation of business risks, and useful breakdown of cost, time, benefit/justification	• No mention of system hardening or cleaning the current breach. Though explained well, need to better summarize the strategy and priorities for the C-Suite will help keep within the time limits • In the future, I recommend providing two pricing options for each recommendation to better justify costs. The absence of specific figures and the generality of the ranges did not meet the need for clear cost estimates, which is essential for business leadership's decision-making. • For business risks, it seemed as if external risks were focused on, such as other businesses losing power. This was not tied back to the business in the presentation. Focus on financial risks to the business. • The strategy stated costs as "low", "moderate", etc. Be concrete with costs, using actual numbers. Also provide ROI for those costs. • The priorities provided reasoning that at times bordered on being technical. The C-Suite is not an audience with in-depth technical understanding. Priorities should address business needs, and mention ROI or risks associated with not implementing recommendations. • The presentation was too long. Over 12 minutes, and the task was to make a 5 minute presentation. A C-Suite will not

	appreciate having over twice the amount of time as scheduled taken up. • The presentation at times felt to be a little too informal. It also seemed at times that slides were simply being read off of, and there were too many "uh"s and "um"s. • Ineffective use of time at the beginning; team could have benefited from keeping presentation to assigned ~5min timeframe

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	0	75	25	100	75	50	100	25	50

Whack a Mole	
WAM1	WAM2
281	281

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
1545	20

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
1298