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

DEPAUL UNIVERSITY

DEPAUL UNIVERSITY HAHA TEAM

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 35 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	1000	50.00%	12
Security Documentation	0	0.00%	88
C-Suite Panel	795	79.50%	61
Red Team	1463	58.52%	37
Blue Team	1845	92.25%	55
Green Team Surveys	1189	79.27%	50
Deductions	0		
Overall	**6292**	**62.92%**	**50**

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	1000

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

1	yes	27	no	53	no
2	yes	28	yes	54	Not Answered
3	yes	29	no	55	no
4	yes	30	no	56	no
5	yes	31	no	57	yes
6	yes	32	no	58	yes
7	yes	33	no	59	yes
8	yes	34	yes	60	no
9	yes	35	yes	61	yes
10	yes	36	yes	62	yes
11	no	37	no	63	yes
12	yes	38	yes	64	no
13	yes	39	yes	65	Not Answered
14	yes	40	yes	66	yes
15	yes	41	yes	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	yes	43	yes	69	Not Answered
18	yes	44	Not Answered	70	yes
19	yes	45	yes	71	no
20	Not Answered	46	Not Answered	72	yes
21	yes	47	Not Answered	73	Not Answered
22	yes	48	Not Answered	74	yes
23	yes	49	yes	75	Not Answered
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	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	795

Strong Points	*Areas of Improvement*
• The video is made well and appears professional • This group has a really strong plan for reducing risks in the future - I think the idea of looking into a PPA with a competitor for mutual aid as part of the company's Business Continuity Plan was a really good idea. • Clear and concise presentation besides the hiccup noted below. • The entry does a good job outlining a comprehensive approach to risk mitigation by addressing both immediate and long-term actions. It demonstrates awareness of both technical and business risks, with a focus on practical cybersecurity frameworks like NIST CSF 2.0 and managed security services, which indicates a solid understanding of industry best practices for enhancing security posture.	• The video is too long • For improvement I would suggest reducing the amount of risks/recommendations on the PowerPoint - there were a lot there and none of them were really fleshed out beyond stating what was on the slide. I would also suggest putting some dollar figures in the recommendation section because a lot of the suggests seemed like they would be high dollar solutions (hiring more staff, using a security provider, deploying multiple systems). If that's not the case then a slide or information about the cost could have cleared up how much it would cost the company. • Small hiccup with slides changing and no audio before the second presenter came on, the presentation seemed to end abruptly. Product recommendations could've used more explanation. • The informal tone detracts from the professionalism of the entry. Refining the language and ensuring consistency in terminology would strengthen the impact. Additionally, providing more detailed information on how specific recommendations (like a PPA) would mitigate risks would add depth to the analysis.

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	75	50	50	25	0	75	50	50

Whack a Mole	
WAM1	WAM2
187	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	375

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
1445	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
1189