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

MARQUETTE UNIVERSITY

MU CYBEREAGLES

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 58 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	592	29.60%	57
Security Documentation	552	55.20%	79
C-Suite Panel	978	97.80%	1
Red Team	550	22.00%	85
Blue Team	948	47.40%	91
Green Team Surveys	0	0.00%	87
Deductions	0		
Overall	**3620**	**36.20%**	**87**

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	592

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

1	yes
2	no
3	yes
4	yes
5	yes
6	yes
7	yes
8	yes
9	yes
10	yes
11	no
12	Not Answered
13	yes
14	yes
15	yes
16	yes
17	yes
18	yes
19	yes
20	Not Answered
21	no
22	Not Answered
23	no
24	no
25	Not Answered
26	Not Answered
27	no
28	no
29	Not Answered
30	Not Answered
31	Not Answered
32	Not Answered
33	yes
34	Not Answered
35	Not Answered
36	Not Answered
37	no
38	Not Answered
39	Not Answered
40	Not Answered
41	Not Answered
42	Not Answered
43	no
44	Not Answered
45	Not Answered
46	yes
47	no
48	no
49	Not Answered
50	yes
51	yes
52	yes
53	Not Answered
54	yes
55	yes
56	yes
57	no
58	yes
59	yes
60	yes
61	yes
62	yes
63	yes
64	yes
65	Not Answered
66	no
67	Not Answered
68	Not Answered
69	Not Answered
70	yes
71	yes
72	yes
73	no
74	yes
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	552

Strong Points	*Areas of Improvement*
• The iterative process described in the system hardening was well done. • Thank you for competing in Cyberforce • Good overview and description of hardening steps were well done. • Asset inventory listed all systems and ports in an organized manner. • The system overview was exemplary	• Additional details in the network diagram to show the firewall, internet access, etc • Overall, you needed more detail in all sections. Fully understanding your network helps with discovering the vulnerabilities and base the hardening of those and the basics of system hardening. • The network diagram showed connectivity, but not the logical architecture of the environments. • System overview provided a vague understanding of what the company does overall, but no information regarding systems.

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	978

Strong Points	*Areas of Improvement*
• The outline/agenda following the rubric was very clear. The explanation and specific examples of business financial risks were exceptional. I also liked the short-term and long-term reduction of risks in the same slide. There was detailed reasoning for every decision. Conclusion was succinct, useful, and unique. • I would congratulate the 4 presenters on how professional they acted and spoke, I really feel that they could have presented this to a C-Suite no problem. Presentation was great, I really liked how they had both short-term and long-term HP Recommendations and that the cost to implement them would remain low. • Nice distinction between short-term and long-term strategies and including financial impact	• Though it was good that reasoning behind decisions was very detailed, there were times that explanation ran too long and became unnecessary. Some explanations could have been more succinct, and would have allowed the time to be closer to the 5 minute requirement. • I think the summary at the end could have been shortened, with a presentation this short I don't think a re-cap of the entire thing was absolutely necessary. • Clear acknowledgement of team member contributions • The language could be refined for clarity and professionalism. Certain phrases, such as "we'll be working with financial finance" or "segment critical segment critical networks," are repetitive or unclear and should be revised. Improving

- This entry is well-organized and presents a clear strategy to address the business risks associated with the cyber breach. The outline flows logically, moving from risk identification to strategies and high-priority recommendations. Additionally, it effectively balances immediate actions with long-term plans, and the focus on low-cost, open-source tools is practical and realistic for minimizing expenses.	grammar, reducing redundancies, and enhancing conciseness would make the content more polished and easier to read. Additionally, specifying the names of the open-source tools or providing examples would give the C-Suite more concrete insights into the proposed solutions.

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	50	25	25	25	0	0	0	0	0

Whack a Mole	
WAM1	WAM2
0	0

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
820	128

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
0