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

NEW MEXICO INSTITUTE OF MINING AND TECHNOLOGY

MAGICBYTE

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 57 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	561	28.05%	64
Security Documentation	781	78.10%	61
C-Suite Panel	777	77.70%	65
Red Team	1950	78.00%	9
Blue Team	1995	99.75%	26
Green Team Surveys	1038	69.20%	28
Deductions	0		
Overall	**7102**	**71.02%**	**28**

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	561

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

1	yes	27	Not Answered	53	Not Answered
2	yes	28	Not Answered	54	Not Answered
3	yes	29	Not Answered	55	yes
4	yes	30	Not Answered	56	no
5	yes	31	yes	57	yes
6	yes	32	Not Answered	58	yes
7	yes	33	Not Answered	59	yes
8	yes	34	no	60	yes
9	yes	35	Not Answered	61	yes
10	yes	36	yes	62	yes
11	yes	37	yes	63	yes
12	no	38	yes	64	yes
13	yes	39	Not Answered	65	no
14	yes	40	yes	66	no
15	yes	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	yes	43	Not Answered	69	Not Answered
18	yes	44	Not Answered	70	no
19	no	45	Not Answered	71	Not Answered
20	no	46	Not Answered	72	Not Answered
21	yes	47	Not Answered	73	Not Answered
22	Not Answered	48	Not Answered	74	Not Answered
23	Not Answered	49	Not Answered	75	Not Answered
24	no	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	781

Strong Points	*Areas of Improvement*
• The description of completed/ongoing work in the asset inventory was a nice touch. • Good overview of the system. • Hardening information was extremely detailed and specific. • The System Hardening section is well thought out, however a non-technical reader might find it hard to follow along • The Network Diagram was exceptional for a hand system	• Reduce use of acronyms and/or consistently introduce term before using acronym. • There are common ports like 123 (NTP), that you listed the services as unknown. • For the hardening you should have a specific phased approach for the scenario. • System overview provided a summary of the systems, but lacked how the systems interact with each other. • The report was exceptional, however always consider who the audience is that you're writing to

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	777

Strong Points	*Areas of Improvement*
• The timeline was detailed and realistic. The future risk mitigation and risks of inaction were very clear and concise. Avoided technical jargon and maintained a high-level overview. • I thought the 2 presenters were professional and seemed familiar with the material. I really liked that a timeline was included as a visual. • Described potential financial losses and had nice timeline of strategy implementation • Good idea to mention the average length of a cyber attack, the C-Suite likely wouldn't know that. Taking the potential cost of the cyber breach and breaking it down to cost per hour was a cool way to grab their attention.	• Difficult to see the slides on video. There is description of financial loss due to outages and lawsuits, but specific business financial risks are not identified. Improvements included recommendations amounting to over $150k, which is a lot for a no-to-minimal funding scenario. Minimal reasoning as to why recommendations would enable security and business continuity in the future. • I would recommend not including dollar amounts without explanation of where it came from, a $4.3 million loss was noted in the presentation but I don't know where they got that number from so it seemed like it was meant more for shock value than a credible amount. • Clearer connection of strategies to financial risk

	• "The C-suite isn't seeking spectacle; they're seeking clarity, insight, and results. Remove the distractions, and let the strength of your message stand on its own." - Morpheus, probably.... • It was very difficult to focus on your slides and message with the Matrix projection all over the place. Remember, you're addressing your C-Suite in the middle of a major event, they likely wont have the patience for distraction. Be clear and concise. • Complete a test call before briefing your C-Suite, this will help you identify potential issues to address before the meeting. The volume of your presentation was very low.

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
0	75	75	100	50	100	50	100	100	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
1595	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
1038