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

COLLEGE OF DUPAGE

COLLEGE OF DUPAGE

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 16 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	627	31.35%	53
Security Documentation	803	80.30%	58
C-Suite Panel	957	95.70%	3
Red Team	1031	41.24%	61
Blue Team	600	30.00%	93
Green Team Surveys	525	35.00%	80
Deductions	0		
Overall	**4543**	**45.43%**	**80**

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	627

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

1	yes	27	Not Answered	53	yes
2	yes	28	Not Answered	54	yes
3	yes	29	Not Answered	55	yes
4	yes	30	Not Answered	56	yes
5	yes	31	Not Answered	57	yes
6	yes	32	Not Answered	58	yes
7	yes	33	Not Answered	59	yes
8	yes	34	Not Answered	60	no
9	yes	35	Not Answered	61	yes
10	yes	36	no	62	yes
11	no	37	no	63	yes
12	no	38	yes	64	yes
13	yes	39	Not Answered	65	no
14	yes	40	no	66	Not Answered
15	no	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	no	43	Not Answered	69	Not Answered
18	yes	44	no	70	yes
19	yes	45	yes	71	no
20	no	46	yes	72	Not Answered
21	yes	47	no	73	Not Answered
22	yes	48	yes	74	Not Answered
23	Not Answered	49	yes	75	Not Answered
24	Not Answered	50	Not Answered	76	yes
25	Not Answered	51	yes	77	yes
26	no	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	803

Strong Points	*Areas of Improvement*
• Your system hardening plan has promise! I wish you had more than 1250 words to describe it in more detail. • Calling out time sync in logs was most appreciated, inaccurate timestamps are one of my biggest SIEM pet peeves! • The system overview was thorough and provided a good starting point for the reader to understand the system and the document purpose. • Very well thought out process for system hardening and well documented	• You forgot to put the map box in your inventory and on your diagram. • MapBox VM missing from inventory/diagram. System hardening report could have been a bit more professional toned. • Some jargon used in system hardening section, making it harder for c-suite to follow the information. Remove text from template with instructions for completing template. • Missing MapBox from network diagram

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	957

Strong Points	*Areas of Improvement*
• The two presenters were well-spoken and maintained a strong presence throughout the video including nonverbal body language. Using visual aids is acceptable, but in this case, eye contact was maintained thus increasing the effectiveness of your messaging. The verbal messages were clear, concise, and well-informed. • This presentation was very professional and thoughtful. • Both people looked professional and spoke very clearly. Really easy to understand! • Presentation was very professional	• This presentation could have been improved by mentioning each team member, not just three, by name or possibly adding additional active presenters. In industry, effective teaming is often a key attribute to establishing a pattern of success. Also, assure that the delivery adheres to the allotted time. Time is often the most valuable resource to senior managers, and assuring it is used judiciously will be appreciated. • The time constraint should be regarded. • The slides popping up for one second and then going away was not beneficial. Either longer viewing of slides or none at all. • The video exceeded the allotted time almost to 6 min.

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	50	25	50	0	0	50	0	75

Whack a Mole	
WAM1	WAM2
93	187

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
200	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
525