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

GEORGIA INSTITUTE OF TECHNOLOGY

CYBERJACKETS I

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 26 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	843	42.15%	24
Security Documentation	818	81.80%	54
C-Suite Panel	878	87.80%	33
Red Team	925	37.00%	69
Blue Team	1616	80.80%	71
Green Team Surveys	304	20.27%	66
Deductions	0		
Overall	**5384**	**53.84%**	**66**

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	843

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

1	yes
2	no
3	yes
4	yes
5	yes
6	no
7	yes
8	yes
9	yes
10	yes
11	no
12	yes
13	yes
14	yes
15	yes
16	yes
17	yes
18	yes
19	yes
20	yes
21	yes
22	Not Answered
23	yes
24	no
25	Not Answered
26	Not Answered

27	no
28	yes
29	no
30	Not Answered
31	yes
32	yes
33	yes
34	no
35	Not Answered
36	yes
37	yes
38	no
39	no
40	no
41	Not Answered
42	Not Answered
43	Not Answered
44	Not Answered
45	Not Answered
46	yes
47	yes
48	yes
49	Not Answered
50	yes
51	yes
52	yes

53	yes
54	no
55	yes
56	yes
57	yes
58	yes
59	yes
60	no
61	yes
62	yes
63	no
64	yes
65	Not Answered
66	no
67	Not Answered
68	Not Answered
69	Not Answered
70	yes
71	no
72	yes
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	818

Strong Points	*Areas of Improvement*
• The vulnerability list is a strength. • Excellent job in identifying relevant NIST frameworks and incorporating open-source tools into the system hardening process • Great network diagram. • Their security document is technically sound and concise.	• System overview is too technical for c-suite. Pages-long lists of CVEs does not add to the value of the document and may overwhelm the reader. • There are too many individual CVEs listed; for senior leadership - it's best to present a concise, comprehensive overview that highlights the most critical vulnerabilities. • A little more thought needed for the system overview and for system hardening. • Improving their "Asset Inventory" section as they have missed required asset.

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	878

Strong Points	*Areas of Improvement*
• Good use of NIST. • The presentation was professional and visually appealing. The timeline at the beginning was helpful in showing where we've been, where we are, and where we are going. • Your Risks were very well presented, well thought out and at the correct level of technicality. • Effective recommendations and cost mapping contribute significantly to informed decision-making. There was an impressive alignment of business risks with strategic objectives.	• There was to much jargon for the C-Suite level. Your would have been better to say the jargon and explain what it is. • This is a personal preference, but having just the speaker's camera on would be less distracting. • There wasn't a strong link between the risks and your recommendations.. • I suggest utilizing a virtual background to minimize distractions during meetings. Furthermore, it would be beneficial to acknowledge the contributions of each team member.

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	0	100	0	0	0	0	0	0	0

Whack a Mole	
WAM1	WAM2
375	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	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
1600	16

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
304