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

DEFENDING U.S. ENERGY INFRASTRUCTURE

UNIVERSITY OF SOUTH FLORIDA

USF CYBERHERD

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 38 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	1211	60.55%	8
Security Documentation	976	97.60%	5
C-Suite Panel	943	94.30%	6
Red Team	2025	81.00%	5
Blue Team	2000	100.00%	1
Green Team Surveys	1466	97.73%	5
Deductions	0		
Overall	8621	86.21%	5

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	1211

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

1	yes	27	no	53	yes
2	yes	28	yes	54	yes
3	yes	29	no	55	yes
4	yes	30	yes	56	yes
5	no	31	yes	57	yes
6	yes	32	yes	58	yes
7	yes	33	yes	59	yes
8	yes	34	Not Answered	60	yes
9	yes	35	Not Answered	61	yes
10	yes	36	yes	62	yes
11	no	37	yes	63	yes
12	no	38	no	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	yes	68	yes
17	yes	43	Not Answered	69	Not Answered
18	yes	44	Not Answered	70	yes
19	yes	45	yes	71	no
20	Not Answered	46	yes	72	yes
21	yes	47	no	73	yes
22	yes	48	yes	74	yes
23	yes	49	yes	75	yes
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	976

Strong Points	*Areas of Improvement*
• Overall Great Job all around. The team provides a comprehensive and technically sound system-hardening strategy with strong justifications for actions taken. It was well organized. • The documentation as a whole was professional and thorough. The information was provided in an intelligent, yet easy to understand, fashion. • Great job on the well detailed document that went beyond the bare minimum. • offered useful opening statement and removed template prompts which helped the document read as a "real" artifact towards senior leadership audience	• The diagram includes most network components and makes logical sense with clear connections. However, it could benefit from a legend and more standardized symbols. • Entry text in black instead of grey, to help with those hard of seeing on machines. • Organize the system hardening into major sections so that it reads easier. • well done product, appears to meet requirements. nice groupings and use of tables, categorization of vulnerabilities was also helpful to follow.

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	943

Strong Points	*Areas of Improvement*
• The recommendations are thorough and technically sound • Presentation was great. Delivery was smooth, concise, and easier to understand. Clearly showing the 0 cost associated with your high priority recommendations really pulled me into each idea. • The presentation was done very well, and the presentation by each individual was highly professional! • The presenters did a great job on putting all the content in under 5 minutes.	• Nothing found • Consider removing the costs from your stabilize revenue strategy, draw them in with the ideas and how much revenue is at stake. I was drawn into thinking about those costs more than the idea. You have very limited time with the C-Suite, sell them on why contract workers and insurance is a great way to protect revenue. • no comment • This seems pretty close to the finish line.

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	100	100	75	50	50	75	100	100	75

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
1600	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
1466