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

UNIVERSITY OF CENTRAL FLORIDA

CITRONAUTS

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 15 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	1236	61.80%	7
Security Documentation	960	96.00%	9
C-Suite Panel	898	89.80%	22
Red Team	2075	83.00%	3
Blue Team	2000	100.00%	1
Green Team Surveys	1433	95.53%	6
Deductions	0		
Overall	**8602**	**86.02%**	**6**

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	1236

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

1	yes	27	no	53	yes
2	yes	28	yes	54	Not Answered
3	yes	29	yes	55	yes
4	yes	30	no	56	yes
5	yes	31	no	57	yes
6	yes	32	Not Answered	58	yes
7	yes	33	no	59	yes
8	yes	34	yes	60	yes
9	yes	35	yes	61	yes
10	yes	36	yes	62	yes
11	no	37	yes	63	yes
12	yes	38	yes	64	yes
13	yes	39	yes	65	yes
14	yes	40	yes	66	yes
15	yes	41	yes	67	yes
16	yes	42	yes	68	yes
17	yes	43	Not Answered	69	Not Answered
18	yes	44	yes	70	no
19	no	45	no	71	yes
20	Not Answered	46	yes	72	yes
21	yes	47	no	73	Not Answered
22	yes	48	yes	74	yes
23	yes	49	yes	75	yes
24	no	50	yes	76	yes
25	yes	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	960

Strong Points	*Areas of Improvement*
• Quantity of detected and addressed vulnerabilities. • Overall strong entry, the explanations of tools used were a great addition • The network diagram with further explanation is very helpful especially when working with senior leadership. • Very thorough network diagram	• Improve the organization and presentation of your system hardening plans. You may have "ran out of words" when you reached 1250 and didn't go back to reword or revise the section to say everything you wanted to say. • All of the "Open, to be mitigated in the next cycle" comments on known vulns could have been explained better (e.g., when is the next cycle) • Removal of template text describing how long the section should be. • Difficult to find anything that needs improvement. Well done.

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	898

Strong Points	*Areas of Improvement*
• The content was presented at the appropriate level without using jargon. The team has a strong understanding of the actions that should be considered by the management team and projected credibility in doing so. The corporate background material was also a solid addition. • The seriousness of the business risks were properly conveyed. • I appreciated the uniqueness of the video and everything looked professional. • Each points was addressed in detail, the high-priority recommendations were executed very well.	• This presentation could have been improved by reducing the video slightly to adhere closer to the 5 minute target. When engaging senior management, time is often their most valuable resource. Therefore, doing more with less is a critical skill. • The long-term strategies should have been more thoroughly described. Creating a SOC is expensive. • Risks and strategies to reduce those risks should mention more on how the financials are impacted with cyber security ways to mitigate them. • At certain moments, it appeared that you were referencing your notes. I would recommend practicing your future presentations to become more familiar with the material. This will help engage the

	audience through eye contact to enhance your overall delivery.

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	50	50	100	100	100	100	100	75	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
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
1433