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

FERRIS STATE UNIVERSITY

FSU BULLDOGS

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 41 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	461	23.05%	76
Security Documentation	932	93.20%	13
C-Suite Panel	610	61.00%	85
Red Team	1581	63.24%	27
Blue Team	2000	100.00%	1
Green Team Surveys	1457	97.13%	31
Deductions	0		
Overall	**7041**	**70.41%**	**31**

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	461

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

1	yes	27	Not Answered	53	no
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	no	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	no	36	no	62	yes
11	yes	37	no	63	yes
12	no	38	Not Answered	64	yes
13	yes	39	no	65	Not Answered
14	yes	40	no	66	no
15	no	41	no	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	yes
19	yes	45	Not Answered	71	Not Answered
20	Not Answered	46	no	72	Not Answered
21	yes	47	no	73	Not Answered
22	Not Answered	48	no	74	Not Answered
23	Not Answered	49	no	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	932

Strong Points	*Areas of Improvement*
• Everything was well formatted and easy for me to understand. • My highest scored assessment - well done! • Great job on the asset inventory; all hosts are listed with their corresponding IP addresses, accurately reflected in the diagram.	• Could have included more justification with system hardening. • N/A - see the strong point for this entry. • The system overview, while well-worded, could benefit from additional details as it currently feels vague. Expanding on system hardening and explaining the steps taken would also enhance clarity and completeness.

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	610

Strong Points	*Areas of Improvement*
• The risk coverage is thorough • Clear contributions from variety of team members. • The team made great points for the importance of impact on the people rather than just focusing on the impact to the government and business themselves. • Mentions laws and other government agencies without being too technical • Risk of profit loss was mentioned as a business concern. C-Suite is focused on business risks, especially when it comes to financial risks.	• The presentation could have been more professional. The second slide had entirely too much text. • Minimal discussion of business risks, mitigation is not a sufficient strategy to reduece risks • It would be helpful to have large text slides, such as the Potential Risks to Business slide, be broken down into key points for easier understanding and recall throughout the presentation. • Reading directly off slides, slides include stats with no sources. • No acknowledgement of other speakers, transitions without introduction • The strategy addressed immediate risk. The task was to provide long-term action items. • Provide more explanation on labor costs and the ROI. C-Suite will care less about emotional response, they will want hard data and how it affects bottom line. • Please introduce each team member as they speak. Also, try not to have slides

	packed with text that you simply read off of.

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	100	0	50	0	50	75	50	100	50

Whack a Mole	
WAM1	WAM2
375	281

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
1457