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

SAINT CLOUD STATE UNIVERSITY

SCSU HUSKIES

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 77 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	643	32.15%	50
Security Documentation	846	84.60%	45
C-Suite Panel	895	89.50%	24
Red Team	1256	50.24%	45
Blue Team	2000	100.00%	1
Green Team Surveys	282	18.80%	54
Deductions	0		
Overall	**5922**	**59.22%**	**54**

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	643

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

1	yes	27	Not Answered	53	no
2	yes	28	no	54	yes
3	yes	29	Not Answered	55	yes
4	yes	30	no	56	yes
5	yes	31	yes	57	yes
6	yes	32	yes	58	yes
7	no	33	yes	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	Not Answered	38	Not Answered	64	no
13	Not Answered	39	Not Answered	65	no
14	yes	40	yes	66	Not Answered
15	yes	41	no	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	yes	43	Not Answered	69	no
18	yes	44	Not Answered	70	no
19	yes	45	no	71	Not Answered
20	Not Answered	46	yes	72	Not Answered
21	yes	47	no	73	Not Answered
22	Not Answered	48	no	74	Not Answered
23	Not Answered	49	Not Answered	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	846

Strong Points	*Areas of Improvement*
• Of the team's I reviewed this was the strongest. Exceptional visuals, well thought out comments, just great work! • Overall, nice job. Network diagram was great as was the overall formatting and professionalism of the document. • Overall, the report is commendable, particularly the sections on the system overview and asset inventory, which were well executed. • Great organization, plenty of detail provided. • Most of the document is technically sound and concise.	• Nothing to add! • Some more action details were needed for the system hardening and also support why you are doing those actions. • The system hardening section may require further development. It would be beneficial to include strong justification for the steps taken by the team, ensuring that the rationale is clear and reasonable. Additionally, a list of the tools utilized in this process would enhance the transparency and robustness of this section. • The description was good, but could be improved by focusing on the mission rather than the assets. • By adding missing services; improving network diagram by using distinctive symbols.

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	895

Strong Points	*Areas of Improvement*
• Fantastic work on thoroughly covering both the technical and business-related controls! This balanced approach adds great value. • Clearly stated that the identified concerns will affect revenue. Clearly explained the long-term strategies presented. • Strong flow from business risks to strategy • Excellent presentation and a good, well-rounded approach to the scenario. • Good understanding and communication of the scenario.	• Great job on identifying future business risks in the presentation! Moving this section to the beginning and addressing strategies to minimize these risks could enhance the impact even further • Developing alternative clean energy resources is not a relevant suggestion for a security professional to list as a priority or strategy. • High-priority recommendations should be described in greater detail. The three strategy items were very strong, but the immediate recommendations were less clear.

• Good use of graphics - they summarized the risks quickly and clearly and weren't distracting. • Good idea to have BCP for risk reduction, they are crucial tools in today's cybersecurity landscape. • Good understanding of financial costs for solutions •	• It was great! I believe the C-Suite would have been impressed.

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	25	75	50	75	0	50	100	0	100

Whack a Mole	
WAM1	WAM2
281	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	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
282