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

CHICAGO STATE UNIVERSITY

CSU COUGARS

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 18 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	739	36.95%	34
Security Documentation	694	69.40%	71
C-Suite Panel	765	76.50%	70
Red Team	525	21.00%	86
Blue Team	1125	56.25%	88
Green Team Surveys	0	0.00%	86
Deductions	0		
Overall	**3848**	**38.48%**	**86**

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	739

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

1	yes	27	no	53	no
2	yes	28	no	54	yes
3	yes	29	no	55	yes
4	yes	30	Not Answered	56	no
5	yes	31	yes	57	yes
6	yes	32	yes	58	yes
7	yes	33	yes	59	yes
8	yes	34	no	60	yes
9	yes	35	Not Answered	61	yes
10	yes	36	yes	62	yes
11	no	37	no	63	yes
12	no	38	no	64	no
13	yes	39	Not Answered	65	Not Answered
14	yes	40	no	66	no
15	yes	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	yes	43	no	69	Not Answered
18	yes	44	yes	70	yes
19	no	45	no	71	no
20	no	46	yes	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	694

Strong Points	*Areas of Improvement*
• Well defined and justified system hardening • Very good hardening, describing all justifications very clearly. • Fantastic work on the system hardening, document was well put together. • Clear and comprehensive system hardening section.	• Fully identify operating systems. Describe the business purpose of the system for a C-Suite audience. The network diagram could have been more detailed • Not all assets are listed - think beyond just the VMs. • The System Overview, Asset Inventory, and Network Diagram needed a bit more attention, and were missing details. • More professional formatting (e.g. asset table had empty rows).

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	765

Strong Points	*Areas of Improvement*
• Recommendations for business continuity were fantastic, I really like how Nagios is mentioned as network health monitoring often gets overlooked in cybersecurity programs • Great job identifying relevant open-source tools! • Good inclusion of communication and adding additional resiliency for supplying power • The presentation was professional, and the relevant business concerns were identified.	• The AI generated images are certainly more entertaining than most stock photos, but also a bit distracting • Adding high-priority recommendations and identifying a few more business-related risks would enhance the overall impact of the analysis • Volume super low. Too much text on slides. Focus is on monitoring and no system hardening • The strategy presented addressed immediate risks. While it was a good strategy for addressing those risks, the task was to provide long-term action items, such as policy changes, that the C-Suite should implement. • For the priorities, listing the costs rather than simply stating that they are "affordable" will give the C-Suite better information to make decisions.

	• The video was only three minutes long, and using the full five minutes could have helped in expanding upon your tasks.

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	0	0	0	0	0	0	0	0

Whack a Mole	
WAM1	WAM2
0	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	525

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
1125	0

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

0