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

KANSAS STATE UNIVERSITY

KANSAS STATE CDC

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 52 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	854	42.70%	20
Security Documentation	822	82.20%	53
C-Suite Panel	887	88.70%	26
Red Team	1425	57.00%	39
Blue Team	1995	99.75%	26
Green Team Surveys	995	66.33%	34
Deductions	0		
Overall	**6978**	**69.78%**	**34**

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	854

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

1	yes	27	Not Answered	53	yes
2	yes	28	yes	54	yes
3	yes	29	no	55	yes
4	yes	30	no	56	yes
5	yes	31	no	57	yes
6	yes	32	no	58	yes
7	yes	33	Not Answered	59	yes
8	yes	34	Not Answered	60	no
9	yes	35	Not Answered	61	yes
10	yes	36	yes	62	yes
11	no	37	yes	63	yes
12	no	38	no	64	yes
13	yes	39	no	65	Not Answered
14	yes	40	no	66	yes
15	no	41	Not Answered	67	no
16	yes	42	Not Answered	68	Not Answered
17	yes	43	yes	69	Not Answered
18	yes	44	yes	70	yes
19	no	45	yes	71	no
20	Not Answered	46	yes	72	yes
21	yes	47	no	73	Not Answered
22	yes	48	yes	74	Not Answered
23	yes	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	822

Strong Points	*Areas of Improvement*
• The areas you picked for hardening are a good place to start. • Well designed network diagram. • Your summary and asset inventory were very thorough. Overall your report had a professional look. • The presentation of information in the report was very professional and communicated well. • The Network Diagram was clear and easy to read. • In the System Hardening section did a great job of balancing technical information and stating the informational that also works for a non-technical audience. That kind of balance is appreciated by the non-technical audience, such as upper management.	• Revisit your system overview and think of the audience you are writing to, and what the purpose of the system is, and describe that. • System overview not targeted towards senior leadership. • Your network map could have had interactions between the machines and operating systems. Also, you could have focused more on what you were actually doing with the system instead of quoting NIST - C-Suite is going to want to hear what you did and why you did it not so much about the standard behind it. • Having the “helper” text left in the sections of the report is confusing. Upper management will be confused about what the content is and what is not part of the content. I’ve done the same thing, and it got very confusing to management. • If there's time, having a non-technical person review the report and make comments.

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	887

Strong Points	*Areas of Improvement*
• Each point of recommendation was accompanied by the primary goal or risk it tries to accomplish or address. • Three-prong security strategy approach • Very concise presentation with helpful time estimations for recommendations that support decision making. • Reasonable strategies and high-priority actions	• Move the camera back to properly capture the presenters and screen without overlap or cutting either out of the frame. Add a slide regarding the consequences and risks of not following the recommended actions rather than just speaking about them. • Summarizing financial risks • Something very small; I would recommend moving the objects under the television

	during the presentation to reduce distraction. • Even if a SOC uses internal resources, that is not cheap, and more of a long-term plan than an immediate step.

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
75	75	50	75	50	0	75	25	75	100

Whack a Mole	
WAM1	WAM2
187	187

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
1595	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
995