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

UNIVERSITY OF DALLAS

CYBER CRUSADERS

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 19 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	673	33.65%	39
Security Documentation	856	85.60%	43
C-Suite Panel	845	84.50%	44
Red Team	1575	63.00%	29
Blue Team	1490	74.50%	79
Green Team Surveys	193	12.87%	59
Deductions	0		
Overall	**5632**	**56.32%**	**59**

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	673

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

1	yes	27	Not Answered	53	Not Answered
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	yes	60	no
9	yes	35	yes	61	yes
10	yes	36	yes	62	yes
11	no	37	yes	63	yes
12	Not Answered	38	yes	64	no
13	no	39	Not Answered	65	Not Answered
14	yes	40	yes	66	no
15	no	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	no	43	no	69	Not Answered
18	yes	44	Not Answered	70	Not Answered
19	no	45	yes	71	Not Answered
20	Not Answered	46	yes	72	Not Answered
21	no	47	no	73	Not Answered
22	yes	48	yes	74	Not Answered
23	yes	49	yes	75	Not Answered
24	Not Answered	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	856

Strong Points	*Areas of Improvement*
• The system overview included reference to business purpose/function. • Excellent explanation of system hardening. • Fantastic Asset Inventory and Vulnerability tables. • The documentation provided comprehensive information.	• Inconsistent IP addressing. Include all devices on asset list and network diagram. • You missed a VM. (MapBox) • I think a little more time spent on the formatting of the System Hardening and the document template would have helped tremendously. • The documentation could benefit from more careful and professional formatting.

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	845

Strong Points	*Areas of Improvement*
• The visual flowcharts and not reading off the slides was fantastic, shows you've put a large amount of thought into organizing the presentation • The identification and evaluation of business risks(flow chart analysis) in the presentation are fantastic—well done! • Very good visuals for chain of risks • Great job explaining the risks. The proposed strategies were directly related to the risks. The priorities provided information on the costs and the return on investment. Excellent presentation overall, and very professional.	• The high-priority recommendations left me wanting more, it would have been great to see patching or inventory management mentioned • The risk reduction strategy is good; clarifying on how they can addresses all the previously mentioned business risks could make it even stronger. • No mention of how to deal with the current breach • Nothing major to note; well done.

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	50	25	75	25	0	50	50	25	25

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
1090	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
193