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

UNITED STATES AIR FORCE ACADEMY

DELOGRAND

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 34 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	0	0.00%	92
Security Documentation	884	88.40%	31
C-Suite Panel	913	91.30%	15
Red Team	450	18.00%	87
Blue Team	1800	90.00%	59
Green Team Surveys	1365	91.00%	64
Deductions	0		
Overall	**5412**	**54.12%**	**64**

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	0

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

1	Not Answered		27	Not Answered		53	Not Answered
2	Not Answered		28	Not Answered		54	Not Answered
3	Not Answered		29	Not Answered		55	Not Answered
4	Not Answered		30	Not Answered		56	Not Answered
5	Not Answered		31	Not Answered		57	Not Answered
6	Not Answered		32	Not Answered		58	Not Answered
7	Not Answered		33	Not Answered		59	Not Answered
8	Not Answered		34	Not Answered		60	Not Answered
9	Not Answered		35	Not Answered		61	Not Answered
10	Not Answered		36	Not Answered		62	Not Answered
11	Not Answered		37	Not Answered		63	Not Answered
12	Not Answered		38	Not Answered		64	Not Answered
13	Not Answered		39	Not Answered		65	Not Answered
14	Not Answered		40	Not Answered		66	Not Answered
15	Not Answered		41	Not Answered		67	Not Answered
16	Not Answered		42	Not Answered		68	Not Answered
17	Not Answered		43	Not Answered		69	Not Answered
18	Not Answered		44	Not Answered		70	Not Answered
19	Not Answered		45	Not Answered		71	Not Answered
20	Not Answered		46	Not Answered		72	Not Answered
21	Not Answered		47	Not Answered		73	Not Answered
22	Not Answered		48	Not Answered		74	Not Answered
23	Not Answered		49	Not Answered		75	Not Answered
24	Not Answered		50	Not Answered		76	Not Answered
25	Not Answered		51	Not Answered		77	Not Answered
26	Not Answered		52	Not Answered			

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	884

Strong Points	*Areas of Improvement*
• Clear and easy to understand network diagram. • Excellent diagram & known vulns sections, mitigations were very sensible • Perfect network diagram • The system hardening section outlined the specific steps taken to address identified issues and included the tools utilized, clearly demonstrating how each vulnerability was mitigated.	• Include all given devices in the asset inventory. Be sure to include strong justification that speaks to senior leadership (non-technical business people). Maintain consistent table formatting • Vary your paragraph beginnings in the system hardening write-up, make sure same font/style is used throughout all sections of report • System overview was way too technical • I recommend eliminating any instructions included in the original document and ensuring that the font size is consistent throughout.

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	913

Strong Points	*Areas of Improvement*
• The strategy and recommendations were well thought-out • I think so far this team had the best High-Priority Recommendations that addressed current and future needs related to the company's cyber security. I would also like to note that each presenter spoke very succinctly, looked very professional, and sounded like they had rehearsed the presentation prior to recording. • The summary section was helpful and a good overview • This entry demonstrates a clear understanding of the primary risks to the business, especially regarding the impact on reputation, government contracts, and resource allocation. The recommendations such as implementing	• The audio is difficult to hear at times • I think the only thing that could use some polishing is the break-down and slide about the Risks Related to Business. It looked at first like there were only 2 but the second bullet had multiple points - breaking those out as their own bullets would enforce the seriousness of these risks to the audience. • Business concerns seemed to have more technical details than high level concerns to the business • The entry would benefit from more clarity and structure. The information is somewhat fragmented, making it challenging to follow the logical flow from problem identification to solution. Additionally, refining the language and

an intrusion prevention system, improving employee cyber awareness, and reconfiguring the IT team into specialized units are practical and well-suited to address these risks.	eliminating repetitive points would enhance readability. Including a more precise cost-benefit analysis that quantitatively ties costs to expected benefits would strengthen the argument for implementing the recommended actions.

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	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
1400	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
1365