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

EMBRY-RIDDLE AERONAUTICAL UNIVERSITY-PRESCOTT

XORING EAGLES

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 39 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	848	42.40%	21
Security Documentation	924	92.40%	19
C-Suite Panel	873	87.30%	36
Red Team	1525	61.00%	33
Blue Team	1696	84.80%	70
Green Team Surveys	1269	84.60%	27
Deductions	0		
Overall	**7135**	**71.35%**	**27**

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	848

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

1	yes	27	Not Answered	53	no
2	yes	28	yes	54	yes
3	yes	29	no	55	yes
4	yes	30	no	56	yes
5	yes	31	Not Answered	57	yes
6	yes	32	Not Answered	58	yes
7	yes	33	Not Answered	59	yes
8	yes	34	no	60	yes
9	yes	35	Not Answered	61	no
10	yes	36	yes	62	yes
11	no	37	no	63	yes
12	Not Answered	38	yes	64	yes
13	yes	39	Not Answered	65	Not Answered
14	yes	40	yes	66	Not Answered
15	no	41	no	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	yes	43	yes	69	Not Answered
18	yes	44	Not Answered	70	yes
19	yes	45	yes	71	no
20	Not Answered	46	yes	72	yes
21	yes	47	yes	73	yes
22	yes	48	yes	74	yes
23	yes	49	Not Answered	75	yes
24	Not Answered	50	yes	76	yes
25	Not Answered	51	Not Answered	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	924

Strong Points	*Areas of Improvement*
• Great Job. All hosts are listed with detailed IP addresses and services, including port numbers, meeting the 90%+ requirement. • The system hardening section was structured well and helped the c-suite follow the thought process. • entry appeared to include most requirements	• The system overview could have been more organized and detailed. • Different sized font throughout document; remove instructions for sections from template. • It would have been useful to have the team remove the template prompts and present the document as their own, introduction could have been improved with inclusion of the enterprise name. Also would have welcomed a legend on the diagram.

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	873

Strong Points	*Areas of Improvement*
• The video appears professional and well-made. • I felt you made your presentation fit well for your audience. It wasn't rushed, you avoided cyber specific terminally, and when acronyms were used you included the full name. • Slides were professional looking and your speech pattern was relaxed and easily understood. • The presentation looked great. There was maybe one item to look into, video of the presenters.	• Recommendations require additional funding • While a communication plan is good to have, I would really consider if its worth including in this brief. As a member of the C-Suite, I would want this team to bring forward strategies to reduce my chances of needing to use our comms plan. • The presentation was only 4 minutes long, had you used the extra minute you could have expanded on risks and expectations. • Team did not show the faces.

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	50	0	50	25	25	0	0	75

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
1400	296

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
1269