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

BALDWIN WALLACE UNIVERSITY

BW CYBERSEC

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 10 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	1439	71.95%	2
Security Documentation	829	82.90%	50
C-Suite Panel	802	80.20%	60
Red Team	850	34.00%	73
Blue Team	2000	100.00%	1
Green Team Surveys	1410	94.00%	21
Deductions	0		
Overall	**7330**	**73.30%**	**21**

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	1439

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

1	yes
2	yes
3	yes
4	yes
5	yes
6	yes
7	yes
8	yes
9	yes
10	yes
11	no
12	yes
13	yes
14	yes
15	yes
16	yes
17	yes
18	yes
19	yes
20	no
21	yes
22	yes
23	yes
24	no
25	Not Answered
26	Not Answered
27	no
28	no
29	yes
30	yes
31	yes
32	yes
33	yes
34	yes
35	yes
36	yes
37	yes
38	yes
39	yes
40	yes
41	yes
42	yes
43	no
44	yes
45	yes
46	yes
47	no
48	yes
49	yes
50	yes
51	yes
52	yes
53	yes
54	yes
55	no
56	yes
57	yes
58	yes
59	yes
60	yes
61	yes
62	yes
63	yes
64	no
65	Not Answered
66	yes
67	Not Answered
68	yes
69	Not Answered
70	yes
71	yes
72	yes
73	no
74	yes
75	yes
76	yes
77	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	829

Strong Points	*Areas of Improvement*
• I recognize and appreciate the team using the NIST CSF framework for presentation of team's approach to system hardening. Using industry standard references is a vital capability, and they have done so here. Nice use of the information available to you. • Well written approach to system hardening to include a set of plans • Your network map listed the connections for the SQL database and the modbus dialogs, thorough list of vulnerabilities, very professional appearance. • The system overview and hardening sections are well-worded, organized, and accessible, with clear language free of technical jargon.	• This entry omitted one of the intended assets that was to be discovered, a MapBox VM. This also led to an incorrect network diagram and an incomplete list of vulnerabilities and mitigations. • Ommitted the MapBox • When talking with C-suite try to avoid being too technical by simplifying and over-explaining. some mitigations were too vague - i.e. fixed to be good, passwords changed to be more secure (did you create/enforce a password policy?) • Overall, good job. The team missed a few asset inventories and vulnerabilities.

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	802

Strong Points	*Areas of Improvement*
• The detail put into the high priority recommendations were a great addition. • This team owned their script. The quality of presentation is superb and they covered all areas. At conclusion they also reemphasized on the already explained points and summarized it such that everyone could have a full understanding. • The presentation was well thought out. Great work • Great job identifying and showing the risks!	• Relate the strategies to reduce risk back to the business financial risks. • This team did an excellent job. They understood the assignment and delivered. Congratulations on job well done. • If all members had participated in the presentation and also calling out the team ID would have been great. • Slightly too much information on the recommendation slides.

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
100	50	50	100	75	0	25	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
1600	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
1410