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

PURDUE UNIVERSITY NORTHWEST

CYBER ROAR

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 21 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	561	28.05%	64
Security Documentation	922	92.20%	20
C-Suite Panel	900	90.00%	21
Red Team	1181	47.24%	52
Blue Team	1852	92.60%	54
Green Team Surveys	1352	90.13%	36
Deductions	0		
Overall	**6768**	**67.68%**	**36**

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	561

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

1	yes
2	no
3	yes
4	yes
5	yes
6	no
7	yes
8	yes
9	yes
10	yes
11	no
12	no
13	yes
14	yes
15	yes
16	yes
17	yes
18	yes
19	yes
20	no
21	yes
22	Not Answered
23	yes
24	no
25	Not Answered
26	Not Answered
27	no
28	no
29	Not Answered
30	Not Answered
31	no
32	no
33	yes
34	Not Answered
35	Not Answered
36	no
37	no
38	no
39	no
40	Not Answered
41	Not Answered
42	Not Answered
43	Not Answered
44	Not Answered
45	no
46	yes
47	no
48	Not Answered
49	Not Answered
50	yes
51	yes
52	yes
53	no
54	no
55	yes
56	no
57	yes
58	yes
59	yes
60	yes
61	yes
62	yes
63	yes
64	yes
65	Not Answered
66	no
67	Not Answered
68	Not Answered
69	Not Answered
70	yes
71	yes
72	yes
73	Not Answered
74	Not Answered
75	Not Answered
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	922

Strong Points	*Areas of Improvement*
• Excellent asset inventory, very clear and well structured. • The document was well-structured, easy to navigate, and employed appropriate terminology. • Amazing job with vulnerability identification and hardening recommendations! I loved the technical justifications provided behind the hardening. • All the responses have been technically sound and concise.	• System overview was complete, but not at an appropriate level for senior leadership. • I recommend providing additional clarification regarding the system's purpose and explaining how each component collaborates within the system overview. • Your network diagram's clarity and detail as well as adding executive-oriented language to the system overview would help improve the final quality. • Paying attention to typo mistakes before submitting as they have written 2106 instead of 2016 for Windows Server in the "Asset Inventory" section.

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	900

Strong Points	*Areas of Improvement*
• Quality of video, slides, visual aids and presenters. • Very good list of risks and strategy • Too many texts for a presentation slide, less graphics and too long for the amount of relevant information. Over all good. • Amazing! I love the examples used when showing risks and giving solid recommendations! You put thought into each of them and it shows the C-Suite!	• Additional detail linking observed risks with mitigation strategies (policy, procedure, program, etc.) • No mention of system hardening • My recommendation would be to keep presentation slides with fewer bullet points to avoid visual distractions. Besides that Overall, good job. Keep up the good work. • The only thought I have is to slow down on the intro.

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	75	100	50	0	0	0	75	0	50

Whack a Mole	
WAM1	WAM2
0	281

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	252

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
1352