U.S. DEPARTMENT OF ENERGY'S

CYBERFORCE COMPETITION®

DEFENDING U.S. ENERGY INFRASTRUCTURE

PENNSYLVANIA STATE UNIVERSITY

CYBERLIONS

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 28 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	1414	70.70%	3
Security Documentation	978	97.80%	4
C-Suite Panel	825	82.50%	53
Red Team	1925	77.00%	10
Blue Team	2000	100.00%	1
Green Team Surveys	1483	98.87%	4
Deductions	0		
Overall	**8625**	**86.25%**	**4**

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	1414

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

1	yes
2	no
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	no
18	yes
19	yes
20	yes
21	yes
22	yes
23	yes
24	yes
25	yes
26	no
27	no
28	yes
29	yes
30	no
31	no
32	no
33	yes
34	yes
35	yes
36	yes
37	yes
38	yes
39	no
40	yes
41	yes
42	yes
43	yes
44	yes
45	no
46	yes
47	yes
48	no
49	yes
50	yes
51	yes
52	yes
53	yes
54	yes
55	yes
56	yes
57	yes
58	yes
59	yes
60	yes
61	yes
62	yes
63	yes
64	yes
65	yes
66	yes
67	no
68	no
69	no
70	yes
71	yes
72	no
73	yes
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	978

Strong Points	*Areas of Improvement*
• Very complete vulnerability list. Also system overview is at right level. • Strong network diagram; justified and reasonable hardening steps • Their security document is technically sound and concise • Hardening summary is excellent. It is very well organized per area, easy to read, and detailed. It shows both a technical expertise in vulnerability and configuration management area, and in your ability to present technical information in clear and organized manner.	• Hardening could use some more justification of why things were chosen. • System overview and hardening justification could be less wordy • By improving their formatting. • System overview contains a lot of technical jargon that is not suitable for documentation prepared for executive audience.

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	825

Strong Points	*Areas of Improvement*
• Good high priority analysis and detail. • The visual aids were very professionally done and clearly presented the information. • You provided an excellent non-technical overview of the risks. • The team's slides and the presenters' attire were exemplary in professionalism. Additionally, the presentation adhered to an appropriate time frame.	• Brendan speaks way too fast to the point of not understanding the content. You list tools like IDS and firewalls but don't give solid examples. When you speak in jargon to C-suite, you need to explain what it is. Also, list regulatory compliance guidelines. • Some speakers spoke quickly and seemed to be reading from a script. I would recommend practicing with bullets, instead of full sentences to help reduce the "reading from a script" appearance. Also practice speaking a bit slower. Overall, very well done! • While your identification of immediate and long term costs was well thought out, you did not focus on actions that required minimal funding. • I suggest incorporating key takeaway points into the summary slide and eliminating individual bullet points, as

	technical writing usually reserves bullets for multiple items. Additionally, the discussion of risk currently employs vague terminology. I recommend specifying the probability of a threat being realized rather than categorizing it as high, medium, or low.

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	0	100	100	100	50	75	50	50	100

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
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
1483