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

LIBERTY UNIVERSITY

LU FLAMES

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 56 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	536	26.80%	72
Security Documentation	862	86.20%	40
C-Suite Panel	902	90.20%	20
Red Team	1075	43.00%	58
Blue Team	2000	100.00%	1
Green Team Surveys	1223	81.53%	43
Deductions	0		
Overall	**6598**	**65.98%**	**43**

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	536

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

1	yes
2	yes
3	yes
4	yes
5	no
6	yes
7	yes
8	yes
9	yes
10	yes
11	no
12	yes
13	Not Answered
14	yes
15	no
16	yes
17	yes
18	yes
19	yes
20	Not Answered
21	no
22	yes
23	Not Answered
24	no
25	Not Answered
26	Not Answered
27	Not Answered
28	Not Answered
29	Not Answered
30	Not Answered
31	Not Answered
32	Not Answered
33	Not Answered
34	Not Answered
35	Not Answered
36	yes
37	no
38	Not Answered
39	Not Answered
40	no
41	yes
42	Not Answered
43	Not Answered
44	Not Answered
45	yes
46	yes
47	no
48	yes
49	Not Answered
50	yes
51	yes
52	Not Answered
53	no
54	Not Answered
55	yes
56	yes
57	yes
58	yes
59	yes
60	no
61	yes
62	yes
63	no
64	yes
65	Not Answered
66	Not Answered
67	Not Answered
68	Not Answered
69	Not Answered
70	yes
71	Not Answered
72	Not Answered
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	862

Strong Points	*Areas of Improvement*
• Very well done. I liked the formatting of the assets, by keeping it to minimal rows you make the list easier for senior leadership to digest. • The system overview was the most direct and understandable overview I read. Great job! • System hardening was very in depth and detailed. • The System Hardening section content was exemplary and communicated the writer's experience and skills in this area •	• Very minor but the vulnerability list had some different font sizes and types. • Remove instructions from template, condense system hardening section. • System overview provided a vague at best understanding of their importance/role. • Having the “helper” text on the title page was confusing • In the System Overview the phrase “there is a” is used too much • The content in the System Hardening may be slightly hard for a non-Technical reader

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	902

Strong Points	*Areas of Improvement*
• The slides were professional looking and well laid out. • Nice overall presentation, clear & easy to follow • Mentioning the potential for physical damage to the wind turbines is a great point. When the event is cyber related, its easy for the C-Suite to zero in on what's digital. By mentioning the risk of physical damage, you help them take a step back so they can make more informed decisions. • Full notes in next answer.	• There wasn't a slide to induce your team and some of the high priority actions started to get into the weeks. • Clearer summary of business financial risks • Consider adding a team slide, at times it was tough trying to track who did what and who is on the team. • REQUIRED ELEMENTS - 4/4 • RISKS TO CORE BUSINESS - 4/4 • Company risks are quick, persuasive, minimal jargon, bottom line focused - well done • would have liked to see more discussion of specific risk to gov facilities due to degraded energy output • would have liked to see specific numbers, case studies are good for when you don't have specifics for your org

	• oh you have a whole slide of specific risks to gov facilities. EXCELLENT work • STRATEGY TO REDUCE RISKS - 3/4 • i've always seen orgs break out Incident Response and Disaster Recovery plans, so definitely include IR in here as well. not knocking any points for that, kinda inside baseball, just fyi • no specific timelines or cost estimates given • RRP is overall well-thought out and actionable • what training are you giving to non-cybersecurity workers? phishing? data protection? CIP-compliance focused security training? • HIGH PRIORITY RECOMMENDATIONS - 2/4 • network logging - what are 'events that user has'? examples suitable for C Suite are things like "track every time a user logs in, track every website a user goes to, track every file a user opens, etc" • also what tools? security onion, elastic stack, wazuh? timeline, cost estimates? • account permission audit - excellent recommendation, but tools (bloodhound?)/time estimates? • separate admin accounts - good idea, but to consider this as its own thing outside of account permission audit, would really need tools/timeline/cost estimates • network segmentation - yes, user access is important for network segmentation, but what is really really really important here is simply the airgap, which doesn't look at the user level (OSI 7) but the network (OSI 3) or ideally even the physical (OSI 1) layer. • each of these recommendations is a good starting point but needs to be further developed • QUALITY - 4/4 • try to avoid having our video-in-video placed in a way that blocks slides, can't see all of Risk Reduction Plan • YOU CITED SOURCES amazing ty ty • OVERALL - EXCELLENT discussion of risks, proposed mitigations are all solid but need to be further developed as recommendations to C-Suite

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	50	25	0	50	25	0	50	0	50

Whack a Mole	
WAM1	WAM2
93	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	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
1223