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

UNIVERSITY OF SOUTH ALABAMA

DAYZERO CYBER COMPETITION CLUB

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 33 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	611	30.55%	55
Security Documentation	838	83.80%	48
C-Suite Panel	857	85.70%	39
Red Team	1275	51.00%	44
Blue Team	2000	100.00%	1
Green Team Surveys	1442	96.13%	32
Deductions	0		
Overall	**7023**	**70.23%**	**32**

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	611

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

1	yes		27	Not Answered		53	no
2	yes		28	no		54	yes
3	yes		29	Not Answered		55	yes
4	yes		30	Not Answered		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	Not Answered		60	yes
9	yes		35	Not Answered		61	yes
10	yes		36	yes		62	yes
11	no		37	no		63	yes
12	no		38	Not Answered		64	yes
13	Not Answered		39	Not Answered		65	Not Answered
14	yes		40	no		66	Not Answered
15	yes		41	yes		67	Not Answered
16	yes		42	Not Answered		68	Not Answered
17	yes		43	Not Answered		69	Not Answered
18	yes		44	Not Answered		70	yes
19	yes		45	Not Answered		71	Not Answered
20	Not Answered		46	yes		72	Not Answered
21	yes		47	yes		73	Not Answered
22	Not Answered		48	no		74	Not Answered
23	no		49	yes		75	Not Answered
24	no		50	yes		76	yes
25	Not Answered		51	yes		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	838

Strong Points	*Areas of Improvement*
• Easy to read and interpret network diagram • Great hardening methodology, tells a fantastic story of your effort • The system hardening section outlines the specific steps taken to address identified issues and details the tools employed, clearly illustrating how each vulnerability was mitigated. • Good job on the asset inventory and network diagram!	• Ensure all devices/assets are presented. Double-check for small spelling/grammar mistakes. Be sure to write for senior leadership (i.e. non-technical businesspeople) • MapBox was missing from inventory & diagram, would have liked to see more about how infrastructure pertains to business in the system overview • I recommend removing any instructions that were included in the original document and ensuring that the font color is uniform throughout the entire document. • There is room for improvement regarding the purpose for the system overview section and elaborating on the justifications for the steps taken or not taken regarding system hardening.

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	857

Strong Points	*Areas of Improvement*
• The presentation was very professional • Nice job elaborating on the business risks. • Clear slides • The entry provides a comprehensive analysis of the financial risks and potential legal repercussions facing the company in the event of security threats and service disruptions. It identifies specific risks such as client loss, operational costs, and regulatory non-compliance and suggests practical mitigation strategies and high-priority recommendations, such as offering reduced rates, modernizing security	• Risks were not adequately explained • There were distracting noises in the background of the presentation that could have been removed/re-recorded. • Recommendations could've been stronger and focused more on the CIA triad for the business concerns • Providing more detail on the financial impact estimates or potential costs associated with each recommendation would make the entry more robust.

protocols, implementing an improved security monitoring system, and collaborating with regulatory officials. This thorough approach demonstrates a clear understanding of both the immediate and long-term impacts of security risks on the business.	

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	75	50	75	0	75	50	25	0

Whack a Mole	
WAM1	WAM2
281	93

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
1442