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

UNIVERSITY OF ALABAMA IN HUNTSVILLE

HUNTSVILLETECHSUPPORT

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 48 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	556	27.80%	66
Security Documentation	834	83.40%	49
C-Suite Panel	881	88.10%	30
Red Team	700	28.00%	81
Blue Team	1965	98.25%	47
Green Team Surveys	1357	90.47%	49
Deductions	0		
Overall	**6293**	**62.93%**	**49**

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	556

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

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

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	834

Strong Points	*Areas of Improvement*
• Your system overview is written to the correct audience level. • Report was professional looking and easily read, perfect language for C-suite. • The System Hardening section is well written and easily understandable for the intended audience. • The system hardening description was exceptionally well written • The network diagram was clear and easy to understand	• Find a different way to report your asset inventory that doesn't repeat so much information in the table. • There were vulnerabilities missed. In the report it would have been better if you had listed out the hardening action in a more concise way. • It would be helpful to senior leadership to know more about the vulnerabilities with listed CVE IDs. • The PLC graphic in the network diagram is represented as a workstation, which can be confusing. Check the internet or PLC vendor sites for PLC graphics

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	881

Strong Points	*Areas of Improvement*
• The video is thorough throughout • Well designed presentation. Good use of video of speakers embedded within the slides. • All presenters were attired professionally and did not read verbatim from the slides. They effectively utilized the slides to support their presentation of information. • Excellent job focusing on financial risks, such as fines, repairs, and loss of customers. • Great job at explaining the reasoning for the priorities, as well as their costs.	• None found • Second speaker repeated a sentence. It is recommended to review and edit the video section or reshoot if an error is made as to no confuse the viewer. More details needed as to where open source software would be utilized. Will new staffing be needed to implement these initiatives? • I suggest utilizing a virtual background to minimize environmental distractions and ensure that all visuals in the presentation align with the content displayed on each slide. • The strategy could be better explained as to how it would address the businesses financial concerns. • For the priorities, after listing the costs, I would also mention the return on investment.

	• I noticed that it seemed as if you were looking offscreen quite often. Make sure you focus on the camera as you address the 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
100	0	0	50	50	50	100	50	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	300

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
1565	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
1357