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

SOUTHERN UTAH UNIVERSITY

SUU THUNDERBIRDS

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 80 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	845	42.25%	22
Security Documentation	595	59.50%	76
C-Suite Panel	910	91.00%	16
Red Team	1750	70.00%	18
Blue Team	1990	99.50%	32
Green Team Surveys	1451	96.73%	18
Deductions	0		
Overall	**7541**	**75.41%**	**18**

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	845

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

1	yes	27	no	53	yes
2	yes	28	yes	54	Not Answered
3	yes	29	no	55	yes
4	no	30	no	56	no
5	no	31	Not Answered	57	yes
6	yes	32	Not Answered	58	no
7	yes	33	no	59	yes
8	yes	34	yes	60	no
9	yes	35	Not Answered	61	yes
10	yes	36	yes	62	yes
11	no	37	yes	63	yes
12	yes	38	yes	64	yes
13	yes	39	yes	65	no
14	no	40	no	66	yes
15	no	41	yes	67	Not Answered
16	no	42	Not Answered	68	Not Answered
17	no	43	Not Answered	69	Not Answered
18	yes	44	yes	70	no
19	Not Answered	45	yes	71	Not Answered
20	yes	46	yes	72	Not Answered
21	yes	47	no	73	Not Answered
22	yes	48	yes	74	no
23	no	49	Not Answered	75	Not Answered
24	no	50	yes	76	yes
25	no	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	595

Strong Points	*Areas of Improvement*
• Great use of including CVEs in the known vulns results • System hardening has a great beginning steps to securing the network. • Thank you for competing in Cyberforce. • Asset inventory was presented in a nice table, which makes it very easy to read and understand.	• Mitigations and system hardening were a bit lacking, would have loved to see more details • Ensure that everything documented makes sense within the environment. • Overall, more detail and understanding of the systems and the scenario would help you fill out each section. The section that needed the most work was the system hardening. • 1. Network Diagram is hard to read because of the font color choices that you made: green and red font on a black background. You did not lose any scoring points from me on the diagram itself because of your font color choices. However, you lost some points on your Formatting score because of that. Approximately 8% of men and 0.5% of women have red-green color blindness, making it difficult for them to differentiate between red and green. Relying on these colors can make the document inaccessible to users with color vision deficiencies. To enhance clarity, consider using high-contrast colors. • 2. Known Vulnerabilities section is missing many mitigation steps. • 3. The document contains comments from the template, and these comments should have been removed.

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	910

Strong Points	*Areas of Improvement*
• A strong point for this entry was the discussion around organizational risks -	• This presentation could have been improved by utilizing additional time to

business impacts, consequences, and impacts on the financial elements - are each topics that real-world organizations struggle to navigate effectively. As a result, such topics adequately reflect talking points that senior management at every company must receive updates on. Also, the recommendations identified were technically accurate and continue to plague operational systems (in real-life) when not implemented correctly. • It was a very concise presentation allowing for quick key point making. • The financial risks were clearly stated, and the strategy directly addressed the stated risks. • Presentation was very professional. • Good references at the end. • The presenters looked professional in their appearance and spoke clearly.	provide a wider discussion around the strategies to mitigate business impacts. Time is a resource, and when a opportunity to present to senior management arises, a 5-minute presentation should be very close to 5-minutes. In this case, I think the entry left topics unspoken at the cost of brevity. • There was a lot of time left for the team to be able to go into more detail in each of the sections. They made their key points but more details could provide further convincing for C-suite executives. • For recommended priorities, address the ROI and/or risks of failing to implement the recommendations. The presentation was a little short, and extra minute could have been spend addressing those points. Would have made the presentation perfect. • Consider making more eye contact, it appeared the presenters were reading which doesn't provide a good connection to the C-Suite. • Consider the risks to core business address all of the consequences to the business. • Strategies didn't quite make the mark

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	75	50	50	50	25	50	100	25	75

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
1590	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
1451