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

GEORGIA INSTITUTE OF TECHNOLOGY

CYBERJACKETS II

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 65 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	668	33.40%	42
Security Documentation	880	88.00%	33
C-Suite Panel	833	83.30%	49
Red Team	1019	40.76%	62
Blue Team	1765	88.25%	64
Green Team Surveys	1463	97.53%	40
Deductions	0		
Overall	**6628**	**66.28%**	**40**

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	668

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

1	yes	27	Not Answered	53	yes
2	yes	28	Not Answered	54	Not Answered
3	yes	29	Not Answered	55	no
4	yes	30	Not Answered	56	no
5	yes	31	Not Answered	57	yes
6	yes	32	no	58	yes
7	yes	33	yes	59	yes
8	yes	34	yes	60	yes
9	yes	35	Not Answered	61	yes
10	yes	36	no	62	yes
11	no	37	no	63	yes
12	Not Answered	38	Not Answered	64	yes
13	yes	39	Not Answered	65	Not Answered
14	yes	40	no	66	Not Answered
15	yes	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	no	43	no	69	Not Answered
18	yes	44	Not Answered	70	no
19	yes	45	Not Answered	71	yes
20	yes	46	no	72	yes
21	yes	47	yes	73	Not Answered
22	Not Answered	48	no	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	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	880

Strong Points	*Areas of Improvement*
• I appreciate the quality of the network diagram; it is clearly well-executed and easy to follow. Additionally, the asset inventory list is comprehensive and provides valuable information regarding the assets. • The vulnerabilities are comprehensive, and each has a clear mitigation strategy with a detailed asset inventory which includes all necessary devices, IPs, and services • Diagram and legend were clear and easy to understand. • Your System 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.	• While the identification of vulnerabilities is commendable, I noticed that some of the proposed mitigations were lacking in detail. Additionally, the phrasing may not effectively resonate with a senior leadership audience. I believe that enhancing the clarity and emphasizing the strategic significance of each mitigation could significantly strengthen this section. • The diagram includes main components but misses detail on logical connections and minor components • Vulnerabilities were identified, but data was not presented in an organized manner for senior leadership. • For hardening, clarify steps taken during hardening, not during scanning and reconnaissance. Expand on justification for steps taken during hardening. • - You identified a large number of vulnerabilities. However, it is not clear from the mitigation column where you might have too a specific action and where your comments did not lead to any action, such as "contact vendor". "consider increasing", "consider reducing", and similar. • - You added CVEs, but did not provide any descriptions. Majority of people are not familiar with each and every CVE number, so a verbal description of each vulnerability or a group of CVEs would provide more context to determine if mitigation steps match the vulnerability. When you say "apply patch", it is not clear where the patch is applied: OS, application, etc.

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	833

Strong Points	*Areas of Improvement*
• Thank you for quoting national guidelines. • The presentation was well drafted and all speakers were professional. • Very good summary with the heat map on how the risks will be improved • A strong point of this entry is its clear and structured outline that effectively identifies the major risks posed by the cyber breach to Energia Ventosa's core mission. The presentation logically flows from the identification of key areas impacted by the breach such as residential and commercial customers, government facilities, AI-driven data centers, and supply chains to the financial, reputational, and operational risks. This structured approach allows the audience to grasp the breadth of the issue quickly, while the focus on actionable recommendations, including establishing a cybersecurity response team and implementing a zero-trust architecture, demonstrates a proactive and strategic mindset aimed at mitigating risks effectively.	• If you have a slide (your outline), give the audience time to scan it. You gave us less than 4 seconds to look at the content. • when you change presenters, please announce who you are. Also, don't speak so fast. • Explain jargon in an easy to understand format. • What is zero trust and why are you doing it? • What are AI-driven SIEM tools? • Some speakers spoke quickly so it was hard to fully absorb the information being shared. The sharpness of the slides varied throughout, with some slides being blurry and harder to read. I would recommend providing the heat map findings in a different format, as those were kind of hard to follow. Overall, well done! • Labels missing on some graphics. Don't include your student emails and school website • This entry could have been improved by providing more specific details about the proposed cybersecurity solutions and their implementation. While the recommendations are mentioned, elaborating on how each solution (like the zero-trust architecture and automated incident response) would be executed and integrated into existing systems would strengthen the overall proposal. Additionally, quantifying the expected outcomes of the recommendations such as estimated improvements in response times or reductions in potential financial losses would provide a clearer picture of the benefits and ROI of the suggested strategies. Lastly, a brief discussion on the timeline for implementation could offer further clarity on the urgency and feasibility of the proposed actions.

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	25	75	50	0	0	0	0	0

Whack a Mole	
WAM1	WAM2
187	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	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
1365	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
1463