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

EAST TENNESSEE STATE UNIVERSITY

CYBERBUCS

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 23 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	764	38.20%	32
Security Documentation	887	88.70%	29
C-Suite Panel	850	85.00%	43
Red Team	1581	63.24%	27
Blue Team	1825	91.25%	56
Green Team Surveys	1375	91.67%	25
Deductions	0		
Overall	**7282**	**72.82%**	**25**

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	764

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

1	yes	27	no	53	no
2	yes	28	no	54	yes
3	yes	29	no	55	yes
4	yes	30	no	56	yes
5	yes	31	no	57	yes
6	yes	32	no	58	yes
7	no	33	yes	59	yes
8	yes	34	no	60	no
9	yes	35	no	61	yes
10	yes	36	yes	62	yes
11	yes	37	yes	63	yes
12	no	38	Not Answered	64	yes
13	yes	39	no	65	Not Answered
14	yes	40	yes	66	Not Answered
15	no	41	Not Answered	67	Not Answered
16	no	42	Not Answered	68	Not Answered
17	no	43	no	69	Not Answered
18	yes	44	Not Answered	70	no
19	yes	45	yes	71	no
20	Not Answered	46	yes	72	yes
21	yes	47	yes	73	Not Answered
22	yes	48	no	74	Not Answered
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	887

Strong Points	*Areas of Improvement*
• Very good vulnerability list - team got most. • Logical diagram with clear symbols; comprehensive hardening steps for vulnerabilities. • The document was well-organized and formatted, facilitating ease of understanding. Additionally, the team effectively incorporated the appropriate level of technical detail in each section. • Great job presenting suggestions for system hardening, with a defense-in-depth approach and mitigation steps! • The responses were technically sound and concise	• System overview is too technical. Also, missed a VM. • System is defined well, but might be wordy for senior leadership; missing some assets. • I recommend incorporating subsections within the system hardening section to enhance clarity and readability. This can be achieved by adding subsection titles for each system being hardened. • Adding details to your network diagram with better interconnections and refine the system overview to cater more specifically to a high-level executive audience • By adding the missed required services for the "Asset Inventory" section and improving their formatting.

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	850

Strong Points	*Areas of Improvement*
• Thorough explanations of risks • Next response has my full notes taken while reviewing the video. Video was well-made and addressed a wide variety of risks to enterprise, including financial/operational/reputational/legal. However, these were not connected to the risk reduction and recommendations which followed. On their own, these were all interesting ideas that we didn't really get a chance to explore. TL;DR good bones needs more meat • Professional presentation with good pacing and transitions. Business risks were explored and described well and	• No mention of system hardening, focus is on detection • PRESENTATION - 4/4 • full points you did all the things • BUSINESS CONCERN RISKS - 2/4 • no specific numbers given • no real discussion of risks due to degraded energy output or gov outages, just that these could both occur • minimal jargon • RISK REDUCTION STRATEGY - 2/4 • "Constantly monitored" is a bit vague. Will there be a 24/7 cybersecurity hotline/SOC? Will all alerts be actioned

included reference to government facilities. • Great presentation and good points that you addressed	within 60 min? Or does this just mean that the SIEM is constantly receiving logs? • Operational Focus - we already have a focus on protecting our most critical outputs. Would have liked to see something specific, such as which assets are most critical, or how these will be protected differently than other assets. • Again with cross-functional collaboration - which teams? what work? • also, previously identified business risks are not addressed • overall, 2/4. each of these has very good potential but would need much more specific, actionable recommendations to earn full points • RECS - 3/4 • network security monitoring with a free siem is good, i've not heard of this/would personally go for security onion, but this earns the point • backup power solutions is good, but not free, so doesn't count towards Exemplary. • you highlight 'immediately patching critical known vulns' but don't discuss ongoing patching program. also did not properly make the case for zero-trust as opposed to VLANs or principle of least privilege for purposes of reducing severity of initial breach (although a good point!). • phishing education and knowbe4 are both good recs • SIMILAR RISKS • where are you getting these numbers? "According to Wall St Journal/NERC whitepaper/DEFCON talk" is fine. these also are not risks due to degraded energy output • QUALITY - 4/4 • OVERALL - would have liked to see much more specific risks and recommendations. presentation was very polished and professional. • The strategy to reduce risks could be more directly tied to the specific business risks. The funding requirements of all high-priority recommendations wasn't clear (ex: backup generator) • N/A

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	0	75	75	0	50

Whack a Mole	
WAM1	WAM2
281	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
1425	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
1375