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

COLORADO SCHOOL OF MINES

ORESEC

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 63 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	1111	55.55%	10
Security Documentation	862	86.20%	39
C-Suite Panel	933	93.30%	9
Red Team	1813	72.52%	16
Blue Team	2000	100.00%	1
Green Team Surveys	1384	92.27%	8
Deductions	0		
Overall	**8103**	**81.03%**	**8**

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	1111

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	Not Answered	56	yes
5	yes	31	no	57	yes
6	yes	32	Not Answered	58	yes
7	yes	33	Not Answered	59	yes
8	yes	34	yes	60	no
9	yes	35	yes	61	yes
10	yes	36	yes	62	yes
11	no	37	yes	63	no
12	no	38	yes	64	no
13	yes	39	yes	65	Not Answered
14	yes	40	yes	66	yes
15	yes	41	yes	67	Not Answered
16	yes	42	no	68	Not Answered
17	yes	43	yes	69	Not Answered
18	yes	44	yes	70	yes
19	yes	45	no	71	yes
20	no	46	yes	72	yes
21	yes	47	yes	73	Not Answered
22	yes	48	yes	74	yes
23	yes	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	862

Strong Points	*Areas of Improvement*
• Easy to read and understand Network Diagram. • The most prominent strength of this submission was the thorough list of vulnerabilities identified. By including the CVE references, the report builds its credibility and impact. This also inherently informs the system hardening efforts as informed decision making will enable better the use of constrained resources. • The asset inventory and network diagram were commendably prepared, providing comprehensive information that meets the requirements. • The entry demonstrated a comprehensive understanding of system security and hardening practices across various operating systems and machines. It outlined specific actions taken on each machine, such as removing backdoors, updating software, enforcing password policies, and configuring firewalls. This level of detail shows thorough planning, prioritization, and a strong focus on both preventive and detective security measures, which is a valuable strength in any security assessment.	• Include OS version details in the asset inventory. Double-check for small spelling and grammar errors. Recommendations to senior leadership are often more strategic and comprehensive than specific and technical with strong justification. • The subject entry could have been approved by pulling in a standardized structure to the system hardening efforts. This might include a structure such as the categories prescribed in NIST CSF 2.0 - e.g., govern, detect, protect, identify, response, recover. Doing so adds professionalism, but also better enables senior management to apply the mitigations to specific cybersecurity elements of the organization. • The assessment of the system hardening process did not fully meet established criteria. To improve, the team should expand hardening measures by referencing industry standards and provide clearer justifications for all actions taken and omitted. Evaluating the reasonableness of implemented steps is essential to aligning with best practices and identifying gaps. • The entry could have been improved by adding a more structured analysis or summary of the overall security improvements and remaining risks. While the details for each machine are helpful, a high-level summary or a risk assessment at the end could provide a clearer picture of the system's security status after hardening efforts. Additionally, including more insights on monitoring strategies for untriaged assets like the Map Box, or a plan to address these areas in the future, could strengthen the entry's completeness.

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	933

Strong Points	*Areas of Improvement*
• I liked the review of the problem. There was a clear flow that followed the rubric. The timeline was realistic, and the structure of the presentation was easy to follow and maintained a high-level of technicality. • Good overview of the implications of the risks • The strategy and high priority recommendations flowed nicely. Well done. • The entry's standout feature was its structured, strategic approach to risk mitigation. The team identified specific risks to both government and civilian customer bases and recognized the impact these risks could have on Energy Ventosa's reputation and future contract opportunities. Additionally, they provided a logical sequence of strategies for addressing these risks, including contingency planning, employee awareness training, and vendor evaluation. This comprehensive overview, supported by clear high-priority recommendations like employee phishing exercises and adherence to DoE password standards, demonstrated a proactive and layered security approach.	• The first two presenters talked a bit too quickly, making the beginning hard to follow. The mapping of strategies back to specific business risks and the costs of "vender evaluation framework" were not clear. • Volume was highly varied and at some points hard to hear • Quality control - volume was loud and then quiet for different presenters. • The entry could be improved by incorporating more precise details regarding the technical aspects of the proposed strategies. For example, explaining how the open-source software for backups and security training will be integrated with existing systems would clarify the implementation plan. Adding cost estimates beyond "free and open-source software" would also enhance the entry by showing a realistic assessment of potential additional expenses or resource requirements, even if minimal. Finally, tightening up the language and reducing repetitive phrases would streamline the presentation, making it clearer and more impactful for executive audiences.

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	100	100	100	100	50	0	100	100	100

Whack a Mole	
WAM1	WAM2
187	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
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
1384