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

COLUMBIA BASIN COLLEGE

CYBERHAWKS

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 25 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	436	21.80%	77
Security Documentation	881	88.10%	31
C-Suite Panel	716	71.60%	74
Red Team	1094	43.76%	55
Blue Team	2000	100.00%	1
Green Team Surveys	1485	99.00%	42
Deductions	0		
Overall	**6612**	**66.12%**	**42**

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	436

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

1	yes		27	Not Answered		53	yes
2	yes		28	no		54	Not Answered
3	yes		29	Not Answered		55	yes
4	yes		30	Not Answered		56	yes
5	yes		31	Not Answered		57	yes
6	yes		32	Not Answered		58	no
7	yes		33	Not Answered		59	yes
8	yes		34	Not Answered		60	no
9	yes		35	Not Answered		61	yes
10	yes		36	yes		62	yes
11	no		37	no		63	yes
12	Not Answered		38	no		64	no
13	no		39	Not Answered		65	no
14	yes		40	yes		66	Not Answered
15	yes		41	Not Answered		67	Not Answered
16	Not Answered		42	Not Answered		68	Not Answered
17	no		43	no		69	Not Answered
18	no		44	Not Answered		70	yes
19	Not Answered		45	yes		71	no
20	no		46	Not Answered		72	yes
21	yes		47	Not Answered		73	Not Answered
22	yes		48	Not Answered		74	Not Answered
23	Not Answered		49	Not Answered		75	Not Answered
24	Not Answered		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	881

Strong Points	*Areas of Improvement*
• Excellent vulnerabilities list (you got most!) • System hardening is well-executed, and great job on including DAST and additional details like robots.txt for a more thorough approach • Great list of assets and the vulnerabilities where well documented. • All assets listed; vulnerabilities were properly mitigated and hardened	• Your system overview was too technical for the c-suite. • Consider enhancing the formatting and refining the network diagram for improved clarity and a cleaner presentation • More detailed steps needed for system hardening. • Diagram could use additional symbols/legend; some formatting issues (extra blank pages, diagram could be more centered)

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	716

Strong Points	*Areas of Improvement*
• Very good to start with real-world related incidents! • Full notes in next answer. Really appreciated the 'similar historical breaches' section for discussion of risks posed by degraded energy output • Active participation from all presenters • Great presentation and good points that you addressed	• The idea of including a cost-benefit analysis was good, but there was no discussion of the actual cost of recommendations; some of the recommendations would be expensive and not within the "minimal funding" specified. • PRESENTATION - 4/4 • full points you did all the things • BUSINESS CONCERN RISKS - 2/4 • Would like to see concrete numbers during this section • Excellent breakdown of each risk • No mention of Area of Responsibility or specific risks due to degraded energy output • Minimal jargon • RISK REDUCTION STRATEGY - 3/4 • +1 for Cisco Secure Awareness Training as free phishing prevention • Monitoring 3rd party users - good suggestion, but no specific tools given

	• Good to call out Principle of Least Privilege, but how will access be restricted? • +1 for Incident Response, including specific callout about required content. would like to see more of that • HIGH PRIORITY RECOMMENDATIONS - 2/4 • Firewall - good recommendation, but which firewall? where should it sit? how should we harden it (can you give examples to C Suite of things that could be newly filtered?) • Security Updates and Backup Data - why are these connected? these are two separate controls. which tools? how will these protect against "evolving threats" in a way that a well-filtered firewall or similar controls wouldn't? • +1 for passwords and MFA. called out brute force and specific need for MFA. again, would have appreciated specific tools or which systems will be put behind MFA. • SIEM (always heard it pronounced like The Sims fyi) - how is this a critical component of a data security strategy? • COST BENEFIT ANALYSIS • Glad to see concrete numbers, would like to see sources for those estimates ("from WSJ/NERC Whitepaper/DEFCON talk" is fine) • QUALITY - 4/4 • Describe how impact to government facilities impacts the business, and specifically describe how the proposed strategies reduce this (and other identified) risks. Provide cost estimates for high-priority recommendations. Professional dress-code. • expand more on your risks related to business and high priority recommendations

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	50	75	25	25	50	50	0	100	75

Whack a Mole	
WAM1	WAM2
93	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	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
1485