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

WHATCOM COMMUNITY COLLEGE

ORCAS AGAINST PHISHING

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 61 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	280	14.00%	89
Security Documentation	252	25.20%	86
C-Suite Panel	772	77.20%	66
Red Team	1088	43.52%	56
Blue Team	1810	90.50%	58
Green Team Surveys	1168	77.87%	67
Deductions	0		
Overall	**5370**	**53.70%**	**67**

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	280

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

1	yes	27	Not Answered	53	Not Answered
2	yes	28	Not Answered	54	no
3	yes	29	Not Answered	55	yes
4	yes	30	Not Answered	56	no
5	yes	31	no	57	yes
6	yes	32	Not Answered	58	yes
7	yes	33	Not Answered	59	yes
8	yes	34	Not Answered	60	no
9	yes	35	Not Answered	61	no
10	yes	36	Not Answered	62	yes
11	no	37	yes	63	yes
12	Not Answered	38	no	64	yes
13	yes	39	no	65	Not Answered
14	no	40	no	66	Not Answered
15	no	41	Not Answered	67	Not Answered
16	no	42	Not Answered	68	Not Answered
17	Not Answered	43	Not Answered	69	Not Answered
18	yes	44	Not Answered	70	yes
19	Not Answered	45	Not Answered	71	yes
20	Not Answered	46	Not Answered	72	yes
21	yes	47	Not Answered	73	Not Answered
22	Not Answered	48	Not Answered	74	yes
23	Not Answered	49	Not Answered	75	Not Answered
24	no	50	Not Answered	76	yes
25	Not Answered	51	yes	77	yes
26	Not Answered	52	Not Answered		

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	252

Strong Points	*Areas of Improvement*
• Your network diagram was strong, only missing 1 thing. • Network diagram looks good • Great asset inventory.	• Ignoring missing components. System overview was too technical for a c-suite. Also, you had good content in the asset list, but the structure of the data made confirming that challenging. • Try to complete the entire document • I appreciate the fact that you turned something in. Allocating more time to this task will enable you to answer more questions next year.

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	772

Strong Points	*Areas of Improvement*
• I like the details of your slides. You both spoke very clearly and did not use jargon. • Good idea to add customer risks • Very nice flow • This entry excels in its comprehensive breakdown of risk categories—financial, legal, and reputational and in its cost-benefit analysis. The presentation offers clear, measurable comparisons between the costs of implementing security measures versus the potential losses due to an outage. This approach strengthens the case for investment in cybersecurity and underscores the financial prudence of taking preventive action.	• The strategy for risk management slide needed work for the presentation. The shapes are blocking words. • No video of members • leveraging existing tools - what are they ? • response plan - how and what are you going to do? How are you going about streamlining it? • Need more actionable details overall. • There are compliance agencies that the business must follow. Your action items should reflect their guidelines. • Too much info packed into slides and skipped over the content. Summarize more. • Some minor issues with presentation quality including a click/build that wasn't addressed. • To enhance the entry, the team could further develop specific mitigation steps for each risk category, linking them directly to their outlined high-priority actions. This would add clarity and coherence by

	showing how each recommendation directly addresses a particular risk. Additionally, providing more details on each team member's role and expertise within the project would add to the presentation's professionalism, reinforcing the team's credibility and the strength of their 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	50	50	75	75	0	0	0	50

Whack a Mole	
WAM1	WAM2
187	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
1410	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
1168