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

OREGON STATE UNIVERSITY

OSUSEC 2

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 27 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	707	35.35%	38
Security Documentation	932	93.20%	13
C-Suite Panel	816	81.60%	55
Red Team	1756	70.24%	17
Blue Team	1995	99.75%	26
Green Team Surveys	1365	91.00%	17
Deductions	0		
Overall	**7571**	**75.71%**	**17**

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	707

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

1	yes	27	no	53	yes
2	yes	28	no	54	Not Answered
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	yes
10	yes	36	yes	62	yes
11	yes	37	no	63	yes
12	no	38	no	64	yes
13	yes	39	Not Answered	65	no
14	yes	40	no	66	Not Answered
15	yes	41	yes	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	no	43	Not Answered	69	Not Answered
18	yes	44	Not Answered	70	yes
19	yes	45	yes	71	yes
20	no	46	yes	72	yes
21	yes	47	no	73	no
22	yes	48	no	74	yes
23	no	49	yes	75	yes
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	932

Strong Points	*Areas of Improvement*
• System overview is at exactly the right level for leadership, but could have used some explanatory/extra info (you had word count to spare, use it!) • Strong, clear diagram; vulnerabilites and mitigations were comprehensive and justified. • The content of the security document is technically sound and concise. • Your System Hardening summary is good. It is very well organized per area, easy to read, and detailed. It shows technical expertise in vulnerability and configuration management area.	• Check your formatting - you swap randomly to new font/grey color/size, etc. • System is defined and explained, but does not target senior leadership in a presentation; formatting issues (extra blank pages in document, extra unused rows in vulnerabilities table). • By improving the formatting as the response for "System Hardening" seems copy-pasted from another document. • The document contains comments from the template, and these comments should have been removed.

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	816

Strong Points	*Areas of Improvement*
• I like that the presenters were in the same video and you have some good ideas. • The clear description and expansion of each bullet was easy to follow for all persons regardless of existing cybersecurity knowledge. • You provided good non-technical explanations of the technical terms you used on the slides. • The team compiled a comprehensive list of all members and recognized the unique contributions of each individual. They effectively connected the training outcomes with the cost per employee, providing valuable context for understanding the overall impact.	• More detailed information on your strategic plan, what you are going to do, when, and how long that take. Think like a Gantt chart to show the executives. The presentation felt like you were reading from the screen. When addressing C-Suite, it should be more natural. • Presenters would benefit from additional practice with public speaking. They did a great job here, but further practice will help them be less rigid and build more rapport with the audience. • I didn't see a good connection between your risks and recommendations. • I suggest including key takeaway points in the conclusion slide.

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	50	100	100	75	100	50	25	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
1595	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
1365