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

UNIVERSITY OF RHODE ISLAND

RHODE RUNNERS

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 72 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	672	33.60%	40
Security Documentation	840	84.00%	47
C-Suite Panel	881	88.10%	30
Red Team	700	28.00%	81
Blue Team	1014	50.70%	90
Green Team Surveys	0	0.00%	84
Deductions	0		
Overall	**4107**	**41.07%**	**84**

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	672

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

1	yes	27	no	53	no
2	yes	28	no	54	Not Answered
3	yes	29	no	55	yes
4	yes	30	no	56	yes
5	yes	31	yes	57	yes
6	yes	32	yes	58	yes
7	yes	33	yes	59	yes
8	yes	34	Not Answered	60	no
9	yes	35	no	61	yes
10	yes	36	no	62	yes
11	no	37	yes	63	yes
12	no	38	Not Answered	64	yes
13	yes	39	no	65	Not Answered
14	yes	40	no	66	Not Answered
15	yes	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	yes	43	no	69	Not Answered
18	no	44	Not Answered	70	yes
19	yes	45	Not Answered	71	yes
20	Not Answered	46	yes	72	yes
21	yes	47	no	73	no
22	no	48	yes	74	no
23	yes	49	no	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	840

Strong Points	*Areas of Improvement*
• Good plan for system hardening. • Excellent network diagram and hardening sections. • System overview and asset inventory was well done. • Well thought out and executed hardening guide • Clear, defined system overview; justified and reasonable hardening steps.	• Some more discovery was needed on your network with good documentation. • A bit more time could have been spent on identifying Vulnerabilities, otherwise fantastic work! • The known vulnerabilities section needed to identify most vulnerabilities with appropriate mitigation strategies. Additionally, the system hardening section needed justifications for implementing measures. • Try to close all vulnerabilities you found, and you could have found many more • Missing hosts/details from asset overview and diagram; could add more vulnerabilites identified.

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	881

Strong Points	*Areas of Improvement*
• An attempt at linking risks to business impact is appreciated. • The team presented professionally, with all presenters appropriately attired and actively engaging with the audience rather than reading directly from the slides. The use of slide layouts, shapes, and color effectively enhanced the communication of key points. • Great job with closing out on the risk of in-action. This leaves the listener with a sense of urgency! • The presentation was polished and business effective and the team spoke to the issues, consequences and solutions. The slides were well designed, with no distracting pictures or graphics and they	• Linking the mitigation and remediation strategies to the risks identified. • I recommend providing a detailed list of specific products along with their associated costs to assist the C-suite in making an informed decision regarding the organization's budgetary capabilities. • I had a tough time following your recommendations when they were immediately followed up with the next slide. It left me as the listener wondering what the difference and distinction was. • The presentation was great, however I have a few small suggestions you may want to consider for further presentations: • The sound was muddy, which was distracting. Perhaps have a final preview

didn't resort to using bullet points in order to group information. This kept the message clear. • If I could, I would give bonus points for including the brief on Business Continuity. This is an essential tool to have for resilience of the organization in today's cybersecurity landscape. • The presenters were clear and had no distraction which could come from repeating words, clearing the throat, etc.	of the presentation before giving it, which would help pick up the "little" things" so they can be adjusted before giving the presentation. • It seemed like the presenters were reading from a script, which impacts the audiences as if they weren't being addressed and had no eye-contact. • I liked the idea of the acronym LOSSES, however it seemed like a program and may have been distracting instead of contributing to the purpose of the presentation. • High-Priority Recommendations: While tools may be free there are still resources needed from the company, including salaries and other business resources so it's good to acknowledge that with the c-suite and improves credibility. • I heard a "hey there" at the beginning, which was probably too familiar and not appropriate. •

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
0	50	25	0	50	0	0	50	25	50

Whack a Mole	
WAM1	WAM2
0	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
1010	4

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
0