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

GOVERNORS STATE UNIVERSITY

GOVSTATE2

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 93 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	435	21.75%	78
Security Documentation	215	21.50%	87
C-Suite Panel	430	43.00%	92
Red Team	300	12.00%	91
Blue Team	1200	60.00%	85
Green Team Surveys	236	15.73%	90
Deductions	0		
Overall	**2816**	**28.16%**	**90**

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	435

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

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

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	215

Strong Points	*Areas of Improvement*
• Thanks for turning in something. The asset inventory included the correct number of VMs. • This was submitted two days after the late submission deadline. The numerical scores were cut in half.	• System hardening is about large efforts (e.g., patching, user management, policies) to secure systems, whereas your write-up focused on patching a few key vulnerabilities. •

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	430

Strong Points	*Areas of Improvement*
• A strength of this entry were the technical recommendations to recover from such an incident. The examples listed by the project team mirror those that a real-world management team would need to receive updates on to effectively lead a company back from the stated consequences. In this way, the mock update was effective, impactful, and great experience. • The team demonstrated a high level of professionalism in their attire, and the presentation slides were designed with clarity and simplicity. The presenters articulated the content effectively, focusing on the implications of their recommendations rather than simply reading from the slides. • Good well thought out strategies • Good considerations of legal and incident response measures	• This entry could have been improved by shortening the update as well as involving additional team members. Time is a critical resource for senior managers, and providing an effective update within the time allotted is a necessary element. In this case, the entry went long, thus consuming more than the allocated resources. • The video exceeded the designated time limit. I recommend condensing certain sections to ensure that the presentation remains within the allocated time. Additionally, I suggest including a slide to acknowledge all team members and their contributions. It would be beneficial to incorporate risk probabilities to aid leadership in understanding the quantifiable impact. Lastly, consider referencing specific software options along with their associated costs to clarify the financial resources needed for each recommendation. • Need justifications for actions, and actions need to be actionable • Overall, the presentation did not target C-Suite audience (more tactical/operational

	in logistics), and could have benefited from greater practice or refinement of presentation before final submission.

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	0	0	0	0	0	0	0	0	0

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	300

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
1200	0

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

236