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

UNIVERSITY OF CALIFORNIA-BERKELEY

SEISMICS

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 78 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	376	18.80%	83
Security Documentation	880	88.00%	33
C-Suite Panel	956	95.60%	4
Red Team	1006	40.24%	67
Blue Team	1971	98.55%	44
Green Team Surveys	1269	84.60%	46
Deductions	0		
Overall	**6458**	**64.58%**	**46**

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	376

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	no
4	yes		30	Not Answered		56	no
5	yes		31	yes		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	Not Answered		62	yes
11	yes		37	yes		63	yes
12	Not Answered		38	Not Answered		64	yes
13	Not Answered		39	Not Answered		65	Not Answered
14	no		40	yes		66	no
15	Not Answered		41	Not Answered		67	Not Answered
16	Not Answered		42	Not Answered		68	Not Answered
17	Not Answered		43	Not Answered		69	Not Answered
18	Not Answered		44	Not Answered		70	no
19	no		45	no		71	Not Answered
20	Not Answered		46	no		72	Not Answered
21	no		47	no		73	Not Answered
22	yes		48	yes		74	Not Answered
23	Not Answered		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	880

Strong Points	*Areas of Improvement*
• Clear, professional writing and formatting. The system hardening section was particularly strong. • You have a good foundation. • I appreciate the additional items added to the inventory list. • Professionally formatted document with well described asset system topology.	• The system overview could have been more specific to the system in question, instead of such a high level overview of cybersecurity. However, depending on the background of the senior audience, this could actually be a strength! • The system overview did not describe the system. There were no systems mentioned or what their purpose is. • Ensure that there is strong justification for why you took the hardening steps. I know why, but it needs to be explained out. • System overview felt a bit too specific to cybersecurity. Senior leadership (business people) often need broader context of how systems & assets impact the overall business. Some mitigations may be too technical for senior leadership

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	956

Strong Points	*Areas of Improvement*
• This entry offered a strong visual presentation, confident speakers, and technically accurate content. The team offered solutions that are both applicable to this scenario as well as real-world events. Areas that were uniquely well emphasized include risk management concepts, priority ratings, recommendations, and identifications of business risks and solutions. These are all topics that senior managers are focused on and must receive quality updates. I also want to recognize the team for presenting a strong summary in less time. Given the responsibilities of senior	• One specific element that could have been improved is to add a team introduction and acknowledgement at the start of the presentation. A shorter introduction later, for example at the change of speakers, is included, but the up front attribution is often preferred. • I would have liked to see more specific recommendations with specific cost/details. • The long-term strategies need to be clearly linked to identified business risks. • The font may have been a bit small.

management, time is often the most valuable resource and must be used judiciously. • They were concise, efficient, and effective in their presentation. • Very clear and thorough. Excellent use of the time. • Good explanation of the impact to the control systems - very reassuring to the C-Suite that you understood the problems to the Industrial Controls Systems - I wish I could give you bonus points for that! • The presentation had a strong introduction that contributed to the continuity of the presentation. • Good understanding and communication of the scenario. •	

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	50	50	25	50	0	25	25	0

Whack a Mole	
WAM1	WAM2
281	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
1595	376

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
1269