

UNIVERSITY OF CALIFORNIA-BERKELEY

HOT MICS

November 9, 2024

In-Person

Number of Teams	Max Team Points	Min Team Points	Mean Team Points	Total Points	
Number of reams	Received	Received	Received	Possible	
94	9153	1350	6115.31	10,000	

TEAM 47 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	652	32.60%	45
Security Documentation	816	81.60%	55
C-Suite Panel	842	84.20%	46
Red Team	450	18.00%	87
Blue Team	2000	100.00%	1
Green Team Surveys	271	18.07%	73
Deductions	0		
Overall	5031	50.31%	73

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 | 652

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

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

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 | 816

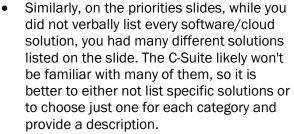
Strong Points Areas of Improvement Thorough investigation of vulnerabilities. Review documents before submitting. Senior leadership will not typically tolerate in the system overview good description of empty pages, constantly changing fonts, what is going on in the system and how they interact, explained acronyms. and poor formatting. thorough explanations on hardening Blank pages took away from the techniques professionalism of the report. Network Diagram didn't show connections to The System Overview and System Hardening sections are well written and router, Didn't list services or OS, didn't straightforward for the intended audience. have a legend More details on the network diagram, All systems were identified in the system such as IP addresses of each system The system overview was well written and would be helpful rather than just listing clear the subnet. Good description of vulnerabilities and The network diagram is clear however remediations consider the technical background of the audience in understanding the diagram. The system hardening description could have been more concise and clear by removing the word"we"

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 | 842

Strong Points	Areas of Improvement
 The risk and strategy portions were thorough The presentation slides created by this team were polished and straightforward, facilitating a clear focus on their messaging. Excellent job on tying the strategy to the annualized loss expectancy. Overall, well-rounded presentation. Team provided specific risks, clear, concise applicable strategy recommendations, and strong example of particular business impact 	 The video was a bit short. More detail could have gone into the recommendations portion. I suggest including the costs associated with each recommendation, as it is important to note that the C-Suite may not be aware that open-source options do not necessarily imply zero cost. For business concerns, the C-Suite may not be familiar with SCADA/ICS, it's better to provide a brief description or explanation. Overall, be more concise with business concerns.



- Your video was only 4 minutes, you were allotted 5. The extra minute could have been used to expand upon reasoning for the priorities, as well as the costs and ROI associated with those priorities.
- Presentation allotted time for additional impact examples with remining ~1min.

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									
Ī	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	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	Al Algorithm Score	
1600	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
	271	