



UNIVERSITY OF CALIFORNIA, BERKELEY

HOTMICS

November 15, 2025

In-Person

Number of Teams	Max Team Points Received	Min Team Points Received	Mean Team Points Received	Total Points Possible
93	8,783	1,267	6,146.81	10,000

TEAM 49 SCORECARD

This table highlights the team's efforts for the 2025 CyberForce Competition®.

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	0	0.00%	93
Security Documentation	695	55.60%	90
C-Suite Panel	572	45.76%	93
Red Team	0	0.00%	91
Blue Team	0	0.00%	93
Green Team Surveys	0	0.00%	93
Deductions	0		
Overall	1267	12.67%	93

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. This year, challenges were longer, and some required more than one person to answer, effectively requiring teams to evaluate risk versus reward.

Anomaly Score | 0

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

1	
2	
3	
4	
5	
6	
7	
8	
9	
10.1	
10.2	
10.3	
10.4	
10.5	
10.6	

10.7	
10.8	
10.9	
11.1	
11.2	
11.3	
11.4	
11.5	
11.6	
11.7	
12	
13	
14	
15	
16	

17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27.1	
27.2	
28	
29	
30	

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 | 695

Strong Points	Areas of Improvement
<ul style="list-style-type: none">Thorough document. Well thought out. Obvious technical expertise.Network diagram is clear and consistent with asset inventory.The network diagram was clear and to the point with the necessary information.Asset inventory included all componentsCovered great amount of details with clarity and looking good to present. Overall great effort by the team.	<ul style="list-style-type: none">Too much jargon in system overview (HMI, PLCs, IPs). Recommend table lines in Asset Inventory; missing services. Incorrect subnet (/26), no symbol for router in legend. Recommend table lines in vulnerability listing; use names vice IPs in host column. Hardening steps appear to be straight from your plan of action and it would be hard for senior leadership to follow.Understand details of asset inventory more . Use provided template and follow rubric. Include justification of hardening steps.

Strong Points	Areas of Improvement
	<ul style="list-style-type: none"> The system overview was not written in a higher level what would be geared towards senior leadership. The system hardening sections listed specific actions that were taken, but did not give a broad overview of what was done to harden the system, nor did it give justification for the mitigations steps that were taken and why some were not taken. The report also did not use the provided template. Content covered was not technically sound or professionally presented (template) Formatting of tables and some clarity in the table content would help in readability. N/w diagram is missing legends and correct symbols.

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 | 572

Strong Points	Areas of Improvement
<ul style="list-style-type: none"> "Unknowns" = excellent point. My other 12 graded teams did not include this. Converted barrels to \$ but would have done that one slide earlier. Decision slide - you want the C-Suite to make a DECISION and give you DIRECTION – great ending. Again, nobody had this. The cost/timeline comparison slide was a helpful inclusion for each action recommended. Very good job separating knowns from unknowns. Having an asks section at the end is great, because it gives the C-Suite something to make a decision on. 	<ul style="list-style-type: none"> Team #15 on Slide 1, but graded as Blue0049. Echo in speaker's slides 1 & 2. Pacing was very slow to the point of annoying. 6.5 minute length. Be full of energy and show that with your confidence and quicker speaking pace. Green letters on black background is not easy to read. Don't read the slides - give additional information than what is on the slides. "Our 30 day plan" - this should be a our Day 1 and Day 2 plans - there is a crisis!!! When showing \$\$\$ amounts, use \$K (thousands), \$M (millions) on graphs instead of all of those zeros. This video is approximately 6:43, far over the 5 minute time limit. Too much time was spent with the introduction and going over the incident itself. Both presenters would benefit from more rehearsal prior to recording their parts. Much technical language was used, such as replayed HMI, PLC, ICS uplinks, etc. and without explaining them. Remember the c-suite audience is not all highly technical. Student last names shouldn't be used, just first names (for privacy).

Strong Points	Areas of Improvement
	<ul style="list-style-type: none"> Some of the cost analysis section was inaccurate. For instance, training staff is not zero cost—even if the training materials/instructors are free, staff time costs money. As another example, having a part-time administrator for the logging platform has salary cost involved. The recommended actions weren't connected sufficiently to the risks." Your risks are not really risks if they do not include likelihood. What you've listed are potential impacts. What is the high level strategy to reduce risks? Your immediate actions, while a good actionable roadmap, includes far too much jargon.

RED TEAM SCORING

RED TEAM FLAG INPUTS (ASSUME BREACH & WHACK A MOLE)

This year we will be using **Assume Breach** as part of your Red team score. This will be worth 1,750 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
0	0	0	0	0	0	0

Whack a Mole		
WAM1	WAM2	WAM3
0	0	0

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	ICS Score
0	0

Each team was scanned 27 times throughout the competition. Below identifies your team's number of successful service scans per required service. Each successful scan was awarded 5 points.

SMTP	IMAP	SMB (task)	NFS	SSH	HTTP	WinRM	LDAP	MariaDB	phpmyadmin	SMB (db)
0	0	0	0	0	0	0	0	0	0	0

The ICS Score was determined by the number of barrels you were able to produce during the competition. The max number of barrels a team should be able to produce (+/- slight variance) was 45,000 barrels. There were two periods in which minimal barrels, if any, should have been produced due to significant weather. The total number of points awarded was 515.

No. of Barrels Produced	Percentage of Total Barrels
0.00	0.00%

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

Green Team Survey Comments

- Site didn't come up. Reload didn't help
- 'This site can't be reached'
- The website does not open. Upon opening the website the user is met with a 'This site can't be reached' message.
- Site didn't load
- site cannot be reached
- website cannot be reached.
- This site can't be reached
- site not loading
- "The page didn't open and the error message was below;
- 'This site can't be reached'
- web.blue0049.cfc.local took too long to respond."
- ERR_CONNECTION_TIMED_OUT x3 attempts to access the page
- Site does not load
- Site did not load.
- This site can't be reached
- Could not reach http://web.blue0049.cfc.local Good luck!
- site wont load
- Sorry still down
- website did not load