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

UNIVERSITY OF CALIFORNIA, BERKELEY

SEISMICS

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 78 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	238	15.87%	84
Security Documentation	1019	81.52%	56
C-Suite Panel	1013	81.04%	46
Red Team	125	5.00%	87
Blue Team	1422	71.10%	80
Green Team Surveys	338	22.53%	82
Deductions	0		
Overall	**4155**	**41.55%**	**82**

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	238

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

1	Yes	10.7		17	Yes
2		10.8		18	Yes
3		10.9		19	Yes
4		11.1		20	Yes
5		11.2		21	
6		11.3		22	
7		11.4		23	
8	No	11.5		24	No
9	No	11.6		25	
10.1		11.7		26	
10.2		12		27.1	
10.3		13		27.2	
10.4		14		28	
10.5		15	Yes	29	
10.6		16	Yes	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	1019

Strong Points	*Areas of Improvement*
• Tables are well organized. • Balanced depth and clarity. It reads like a real SOC report. • System overview addressed the entire system and its purpose, rather than just narrating the asset inventory. • Good job explaining the impact of the vulnerabilities in the Known Vulnerabilities section. • The overall presentation.	• System is only briefly described. System hardening was too detailed with specifics of what was done instead of being a broad overview with justification for why mitigations steps were or were not done. • Could include a short summary of residual (unfixed) risks. • It felt like a narrative of the known vulnerabilities chart, rather than preemptive measures and defensive tactics to protect machines and a network. • Be consistent with hostnames. The System Hardening section is meant for writing about

Strong Points	Areas of Improvement
	broad steps or categories of hardening and defense strategy, not explaining vulnerabilities in each machine. • Technical skills and strategic thinking abilities.

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	1013

Strong Points	Areas of Improvement
• Excellent focus on and appropriate level of detail for business risks and operational impacts. • the coverage of the rig classification was too techy, • Good job at measuring the risk levels with low, medium, high, but how did you calculate those? If you used R=L*I, how did you arrive at the likelihoods? You kept the risks in view when talking about strategy. This is very effective way to always make sure you are addressing your risks. • problem statement explained well, all members contributed to presentation, and some of the technical jargon was explained for non technical people. • Risks were directly addressed in your mitigation strategies.	• Cyber-relevant scenario details (e.g. network outage, galley contractor work) were entirely omitted except for in the final slide. Using colloquial language ("dunno why it was connected to ICS") isn't appropriate in this context. • less detail, quantify risks financially & solution cost. too much detail on some of the slides. • Your strategies tie directly back to your risks, but they should be longer term thinking. These mostly read as immediate actions to take. WAY too much information on your slides. Your initial plan of action should have cost estimates. The presentation ends very abruptly. • the video seemed a bit rushed, some points were explained better than others, it was hard to understand the long term actions or repercussions if not followed. It was also unclear on the funding needed to implement their plan. • All these risks affect the bottom line. You need to tell the C-Suite how.

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	125	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
1220	202

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)
18	18	15	26	27	16	27	27	16	27	27

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
17674.64	39.28%

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
338

Green Team Survey Comments
• check your headers, footers, front page, admins, and careers! • a lot of differences. • "The color was yellow. The company name in the main homepage was incorrect 'Obsidian Energi Co.' The tagline was incorrect. No career options were listed. No Admins were listed. No footer on the main homepage. And the company name and the address were incorrect in the footer. No logos are listed." • Site is yellow, tagline is wrong, address does not appear on main page, no logos in header, no careers listed • "site color is green footer is not on home-screen no open positions no header logos The tagline in front of the home background image is different" • Green and blue admin not showing on user management page • This site can't be reached • Site not reachable. • your site is unreachable! • Hello Team 78 I kept getting a 504 Gateway Time-out error. • Your site is down • 4:45 site is down • This page isn’t working