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

ROCHESTER INSTITUTE OF TECHNOLOGY

BRICKFORCEENERGY

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 9 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	468	31.20%	40
Security Documentation	1140	91.20%	24
C-Suite Panel	1089	87.12%	22
Red Team	1500	60.00%	14
Blue Team	1889	94.45%	21
Green Team Surveys	1418	94.53%	9
Deductions	0		
Overall	**7504**	**75.04%**	**9**

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	468

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

1	Yes	10.7		17	Yes
2	No	10.8	No	18	Yes
3		10.9	No	19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	No
6		11.3	Yes	22	
7	No	11.4	Yes	23	
8		11.5	Yes	24	No
9	No	11.6	No	25	No
10.1	Yes	11.7		26	
10.2	Yes	12		27.1	Yes
10.3	Yes	13		27.2	Yes
10.4	Yes	14		28	No
10.5	Yes	15	Yes	29	No
10.6	Yes	16	No	30	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	1140

Strong Points	*Areas of Improvement*
• Good job using sub sections and bolded font to help with readability, for instance in the system hardening section and asset inventory. Also, the vulnerabilities section was quite thorough. • Nice detail and an extensive list of vulnerabilities was provided. • Detail documentation! • Exemplary Hardening Strategy and Justification: The approach to system hardening was strategic, highly professional, and robust. The team framed their defensive procedures using the NIST	• Use black font for better readability in the system overview and system hardening sections. • The network diagram did not show logical connections. • While the diagram accurately depicted all six assets, their technical details (IP, OS, Ports), and their connection to the central router and the Internet, it was missing logical connections and interconnects between the devices. • To achieve an Exemplary score (4) in this section, diagrams must include all logical

Strong Points	Areas of Improvement
Cybersecurity Framework (CSF) 2.0 functions (Identify, Protect, Detect), providing a clear roadmap for security operations. The described steps were comprehensive (4+ steps required for Exemplary), including the use of standards-based configuration (DISA STIGs and SCAP Benchmarks), proactive auditing, and deploying a robust, centralized monitoring solution (OSSEC, a free and open-source SIEM) across all systems, including the assumed breach infrastructure. The justifications provided for these steps were strong, aligning with best practices and well-accepted principles. • Comprehensive Vulnerability Reporting: The team submitted an extensive list of vulnerabilities, identifying a massive number well above the threshold required for the Exemplary category. Crucially, the team provided an appropriate, technically sound mitigation for each vulnerability listed. Furthermore, the team successfully processed the raw vulnerability data into a summarized table format, which effectively targets a ""senior leadership"" audience. • Attention to Detail: The Asset Inventory was meticulously detailed, listing all six required hosts, accurately defining their operating systems (e.g., Windows Server 2022, Ubuntu 22.04, OpenSUSE Leap 15), correct IP addresses, and providing a comprehensive list of associated TCP and UDP ports and services. This demonstrated a full understanding of the system environment.	connections and interconnects between assets on the competition network. For example, the diagram should depict the communication flow showing connections between the Web Server and the Public DB, or how clients (like the HMI or Task Box) interact directly with the AD/DNS server for authentication and naming services. Current and detailed network diagrams, including these logical connections, are essential for enhanced situational awareness, especially when responding to a cybersecurity incident.

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	1089

Strong Points	Areas of Improvement
• kept a good pace of information and speech • High Priority Recommendations that is simple, concise, articulated, and reasonable • Nice high level summary of cost and timeline	• a bit difficult to understand some speakers • They could have had some volume or inflection in their presentation. Add excitement instead of just reading off a script

Strong Points	*Areas of Improvement*
• Fantastic high-priority recommendations, excellent job explaining importance of network segmentation • Your identified risks were clearly summarized, related to business functions, and contained an appropriate level of technicality for the C-Suite.	• Include discussion of future risks in recommendations not followed along with better clarity of which recommendations are long term strategies • It felt like a bit too much time was spent talking about what happened, and not enough on business impact should the new cybersecurity controls not get implemented ASAP • Your strategies could have correlated more directly to your identified risks.

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
250	0	0	125	125	0	250

Whack a Mole		
WAM1	WAM2	WAM3
250	250	250

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
1475	414

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)
27	27	27	26	27	26	27	27	27	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
36207.75	80.46%

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
1418

Green Team Survey Comments
• Great work! Website is fully functional
• The word 'Rift' is missing in the title.
• Header says Obsidian Energy Co instead of ObsidianRift Energy Co
• Good Job
• Excellent work!
• Great job! You secured that oil rig so tight even the crude couldn't slip past you!
• Nice job!
• red user added,
• Site is down