



## NEW MEXICO TECH

### MAGICBYTE

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 59 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	630	42.00%	19
Security Documentation	1109	88.72%	36
C-Suite Panel	979	78.32%	51
Red Team	1125	45.00%	35
Blue Team	1915	95.75%	16
Green Team Surveys	1272	84.80%	31
Deductions	0		
Overall	7030	70.30%	31

## 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.

<b>Anomaly Score</b>	630
----------------------	-----

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

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

<b>Security Documentation Score</b>	1109
-------------------------------------	------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> <li>Both the Vulnerabilities and System Hardening are well developed and thorough.</li> <li>Very professional and kept to the rubric.</li> <li>Good job on the asset inventory and the system hardening.</li> <li>Thorough system hardening plan. Well thought out document.</li> </ul>	<ul style="list-style-type: none"> <li>There are a lot of tools out there that could have been used to create the network map. I really recommend looking into DrawIO a free tool that can allow you to create diagrams.</li> <li>The overview may be a bit lacking.</li> <li>For the system overview, give an overview of the system. What is it intended to do? Why does it exist? What are the components?</li> <li>System overview not written to a senior leadership audience; should be a summary with 2-3 paragraphs. OS for HMI missing. Added SIEM server to network diagram (not</li> </ul>

Strong Points	Areas of Improvement
	allowed); VPN device would be between router and Internet; all devices are outside of subnet listed. Vulnerability listing - use CVE descriptions vice numbers, <23 of built vulns listed.

## 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	979
---------------------	-----

Strong Points	Areas of Improvement
<ul style="list-style-type: none"> <li>• Good presentation! I thought you included some practical details, particularly regarding the strategy to mitigate business risk and the high-priority recommendations.</li> <li>• This is a very good presentation and good plan for the strategy and recommendations. Costs were justified.</li> <li>• Well-defined short- and long-term plan emphasizing quick recovery and staff engagement.</li> <li>• The team provided a summary of the business risks that were addressed in isolation but quantified the impacts to the company's bottom line. They also included a slide dedicated to identifying all members of the team and their hypothetical roles within the response team.</li> <li>• Cost analysis throughout was good. Good for referencing industry standards.</li> <li>• Including communication plan as part of recovery actions and strategy</li> </ul>	<ul style="list-style-type: none"> <li>• Area for improvement regarding risks to core business should clearly identify how these risks affect the company's concerns and bottom line.</li> <li>• one of the presenters had his hands in front of his face which was distracting.</li> <li>• Some redundancy between sections. Analysis doesn't fully differentiate operational vs. business risk. The presentation could be improved by briefly summarizing each recommendation at the end for extra clarity, ensuring the C-suite leaves with a concise list of next steps.</li> <li>• The proposed strategy does provide a reasonable approach to reduce risks moving forward but it does not directly relate to previously identified risks. A simple solution would be to say that business continuity is a risk and that the strategy being proposed would support future continuity.</li> <li>• Risks focused on technical detail not needed for CISO level. No ties between strategies / recommendations to identified risks. Videos of team members presenting was tiny, could not see you!</li> <li>• Recommendations and strategy don't tie back to incident, although they are still good practice.</li> </ul>

## 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	125	125	0	125	0	0

Whack a Mole		
WAM1	WAM2	WAM3
125	250	125

## 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
1460	455

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	24	27	27	26	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
39789.95	88.42%

## 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.

<b>Green Team Score</b>
-------------------------

1272
------

<b><i>Green Team Survey Comments</i></b>
--

- your logos are switched! and, make sure to keep the 'Rift' part of ObsidianRift!
- "The company name is 'ObsidianRift Energy Co. Headquarters.' No space between 'Obsidian' and 'Rift' but your website has the space between. It's a small thing but the company name is important. So I deducted the footer point."
- Company name mistyped, a lot of additional users
- good job
- Didn't load
- your site is not accessible!
- The footer is not on every page. It is missing on the signup and login pages.
- Good job
- Excellent work Team 59!
- "This appears to me a perfect example Slight variation of template where its oil rig footer some water this version is oil rig some water footer slight variation however, meets criteria"
- red team added
- 5:52 This site can't be reached