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

UNIVERSITY OF NEVADA LAS VEGAS

LAYER ZERO

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 58 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	430	28.67%	48
Security Documentation	1156	92.48%	20
C-Suite Panel	1028	82.24%	40
Red Team	750	30.00%	53
Blue Team	1874	93.70%	28
Green Team Surveys	1320	88.00%	45
Deductions	0		
Overall	**6558**	**65.58%**	**45**

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	430

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

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

Security Documentation Score	1156

Strong Points	*Areas of Improvement*
• The formatting was excellent and the explanations were clear. • The addition of the business impact to the known vulnerabilities is great! This really helps the c-suite further understand the vulnerability and why they should care about it being fixed. Defining the methodology used in the system hardening also helps non-technical readers follow what is being described. • Great job on the system overview. It reads well and gives a high level overview of the	• The "urgency tiers" could have been explained before they were first used, this was confusing until I saw how they were defined. • Include information about the breach in the system overview. Mark devices with assumed breach in asset inventory and network diagram. Webserver OS is OpenSUSE Leap. • The system hardening should not be a diary, but a list of steps, with justification, taken to harden each system. These should be

Strong Points	Areas of Improvement
system. Great job giving an impact to vulnerabilities! • Overall this was an extremely strong entry, keep up the good work!	written in a way that is repeatable in the future. • More info on what you'd be doing for log analysis would have been nice

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	1028

Strong Points	Areas of Improvement
• Good job up front establishing the risk and impact. • Strong point for this entry was definitely Business Operation Risks & Impact. This section was neatly laid out with impacts and results clearly stated, calling out financial impacts where relevant. Bottom Line was a nice touch. Great job calling out future business risks. • Good work on including a reference for the risks. • Thorough understanding of regulatory impacts and financial risks, and a framework methodology for risk management. • Great job on the risks and being clear on the financial impact. • Good risk identification and explanation	• Would have liked to see some no cost recommendations. The C-suite is expecting to hear form their cyber team, if you are limited on time try to keep recommendations in your area. Evacuating hazardous areas is something they would hear from WSH. • Less time needed to be spent on the presentation and incident overview. This had a bit too much technical detail and could have been more concise, that would have allowed for more time on more relevant sections regarding recommendations and strategies. High priority recommendations seemed a bit more tactical and responsive in the immediate term, not necessarily focused on remediation but initial "stop the bleed". Would have been beneficial to include other low-cost actions to improve the general security posture. • When introducing the team members recommend also assigning and discussing job roles, job titles, or job duties. • High priority recommendations, include costs, staffing needs and training needs, hardware and software requirements, etc. • Mitigation strategy good use of including costs and timelines. • May be beneficial to include example software and hardware. • Vendor management could be more specific, emphasizing IoT/OT supply chain risks, and recommendations could be linked to measurable outcomes. • Go more in-depth with reasoning for the high priority actions.

Strong Points	*Areas of Improvement*
	• You need to address how each high priority recommendation individually prevents future 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	125	0	125	0	125

Whack a Mole		
WAM1	WAM2	WAM3
0	0	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
1475	399

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
34936.24	77.64%

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
1320

Green Team Survey Comments
• your logos aren't in the right place!
• "Admin button shows up if non-admin logged in. User List when Admin user logged in is blank."
• On every page except the home page the footer moves with the site as you scroll. logos are not transparent
• extra users added, logos not surrounding company name
• footer text has wrong company name and on the top of webpage.
• Recommend changing position of your logos they are located differently from the others it is normally on either side of the company header
• The logos are there but they are in the wrong place, they should be around the company name
• Good job. There were some spelling errors, but all objectives were met.
• Nice work Team 58!
• Rock-solid work! Even Obsidian Rift's rigs approved Unfortunately, your navbar headers are out of regs :(
• You have the logos, but they are in the inappropriate spot within the header. One is at the beginning of the header, and one is in-between careers and ObsidianRift Energy Co. Within User Management, there is a red user that has made its way into the list.
• 5:43 This site can't be reached
• website is down