



UNIVERSITY OF DENVER

DUCRYPTION FORCE

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 42 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	338	22.53%	68
Security Documentation	1003	80.24%	60
C-Suite Panel	984	78.72%	49
Red Team	250	10.00%	82
Blue Team	1887	94.35%	22
Green Team Surveys	1298	86.53%	62
Deductions	0		
Overall	5760	57.60%	62

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	338
----------------------	------------

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

1	Yes	10.7		17	Yes
2	No	10.8		18	Yes
3		10.9		19	Yes
4		11.1	Yes	20	Yes
5	Yes	11.2	No	21	
6		11.3		22	
7	No	11.4		23	
8	No	11.5		24	No
9		11.6		25	
10.1		11.7		26	
10.2	Yes	12	No	27.1	No
10.3	Yes	13		27.2	No
10.4		14	No	28	Yes
10.5		15	Yes	29	No
10.6		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	1003
-------------------------------------	-------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> Summary of tools used was helpful. Asset inventory provided decent detail. Good work! The Vulnerabilities and Mitigations section is very thorough and detailed; additionally, the recommendations in the System Hardening section are excellent, professionally presented and organized for senior management. system hardening is well organized The vulnerability section shows solid research and organization. 	<ul style="list-style-type: none"> Vulnerabilities are focused almost entirely on CVEs - need to include other types and consolidate CVEs into single note. System overview needs to capture the purpose of the system overall. Overall, the document could benefit from improved formatting and aesthetic appeal, as well as enhanced technical detail and explanations. For instance, the system overview section could be strengthened by including additional details regarding system definitions and purposes. Furthermore, the system hardening section

<i>Strong Points</i>	<i>Areas of Improvement</i>
	<p>could be enhanced with a more comprehensive and technically sound set of hardening steps and justifications.</p> <ul style="list-style-type: none"> • The System Overview could be more developed, explaining the 6 systems involved in more detail, possibly categorizing them in IT or OT buckets. The network diagram does contain all the components but needs to be better formatted for presentation to senior management, it looks like the bottom of the network diagram is hidden under a template footer. It's readable but could be improved. • system overview is minimally defined and not geared to senior leadership. Vulnerabilities list is quite short and needs to be looked at a bit more thoroughly. • Tone and content are too technical for a "senior leadership" audience.

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	984
----------------------------	------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> • The high priority recommendations were well done and tied back to the business risks. • I like recommendation 4 but I would consider its value in this specific briefing. The company is under duress, the C-suite is likely getting clobbered, and your CTO / CISO is hearing this brief for the first time. Is this really the right time to imply that there is a lack of leadership level cyber awareness and associating it with this event. Not saying you have to praise leadership but there are a time and place for things so really consider your audience and timing. • Good idea to incorporate KPIs into executive dashboards, but have you thought about how that motivates your IT team? • Very good reasoning for recommendations • Explains the basic path of handling the threat with easy to read slides. Keeps 	<ul style="list-style-type: none"> • Risks addressed in isolation and not summarized as a whole for business and operational risks. Strategy minimally addressed back to the identified risks. The high priority discussion was well done, but the slides had a lot of wording. • No ties between strategies / recommendations and identified risks. • Good strategies, but they need to be more specific. A lot of general statements but not specific implementations and mentioning which risks they mitigate. • Please include some real-life scenarios and provide some open-source tools that would mitigate the risk, create a company wide strategy and maintain the company's integrity

<i>Strong Points</i>	<i>Areas of Improvement</i>
reputational risk as part of the employee training, present and future.	

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
125	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
1435	452

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)
22	24	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
39498.91	87.78%

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

1298

Green Team Survey Comments

- missing users in user management page. footer not included on home page.
- No footer on a Home, no admin users.
- No admin users, no footer on a Home page
- The navigation bar is not formatted. It should span the top of the page. No admin users were listed in the admin page. The footer was not available on every page. The logos appear outside of the navigation bar.
- Logos are in the wrong location and Blue and Green admin users are gone
- Recommend putting footer on the home page and also suggest adjusting the logos as samples show the a logo on each side of the company name
- Logos are too far apart and red user is a admin.
- extra admin account
- Rock-solid work! Even Obsidian Rifts rigs approve" Unfortunately, you've got an extra admin in your ranks and that sticky footer makes it hard to read the whole page.