



DEPAUL UNIVERSITY

SECURITY DAEMONS

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 57 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	513	34.20%	31
Security Documentation	900	72.00%	73
C-Suite Panel	915	73.20%	73
Red Team	625	25.00%	67
Blue Team	1360	68.00%	82
Green Team Surveys	1340	89.33%	64
Deductions	0		
Overall	5653	56.53%	64

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	513
----------------------	------------

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

1	No	10.7	Yes	17	Yes
2		10.8	Yes	18	Yes
3		10.9		19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6	No	11.3	Yes	22	
7		11.4	Yes	23	
8		11.5	Yes	24	No
9	No	11.6	Yes	25	No
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	No
10.5	Yes	15	Yes	29	
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.

Security Documentation Score	900
-------------------------------------	------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> good asset inventory and network diagram. Mentions concrete hardening actions across multiple layers. Nice network diagram and Asset list. Great job on the asset inventory. Great job justifying your hardening steps. System hardening steps were solid! 	<ul style="list-style-type: none"> The overview and vulnerabilities were lacking. Focus on your environment and summarize outcomes. Right now it feels like a generic security essay. System hardening could have been a bit more formatted. "Would like to see more detail in the system overview. Would like to see a differentiation in the network diagram between different types of systems.

<i>Strong Points</i>	<i>Areas of Improvement</i>
	<ul style="list-style-type: none"> In your vulnerabilities, you used terms like "too many admins." This is subjective terminology." The vulns section was severely lacking; would have loved to see far more with CVEs cited

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	915
----------------------------	------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> Appropriate start. Excellent Active Risks slide. I like seeing the Bottom Line clearly defined. Risk was covered well The necessary issues were covered really well. The speaking pace was easy to understand. Risks were clearly defined and correlated to bottom line. Good work including references, nice slide design. 	<ul style="list-style-type: none"> Label speakers on slides. Both speakers need to have ENERGY - consider standing when speaking so you have more air in your lungs. DO NOT read your slides. Give other information. Consider fewer words on your slides so that the audience has to listen to you. Strategy to Reduce Risks slides should have costs for each action, even if \$0. Add separate slide with your applications. Redo the section where you advance the slide too soon. Consider one voice file per slide. "Thank you and we wish you the best of luck" sounds like "we are out of here" - no bueno. Instead, "We are available to answer your questions." Lacked financial impacts/costs information. Lacked timeline for completing the recommendations. Be sure to proof your video ahead of time, your in presentation video circles blocked out some content. The face cam covered information on the slides Strategy connection to risk was not clearly identified One team member presented the majority of the information The image for the presenter got in the way of the slide information. The slides were word heavy, separating the individual headers to their own slides would have giving more talking time, easier to read slides and lengthened the video to five minutes.

Strong Points	Areas of Improvement
	<ul style="list-style-type: none"> Your risk reduction strategies should all be long-term strategies, while the high priority actions should occur in the short term. Cover slide video of speaker covers the slide content. The slide content should be adjusts so that the speaker video does not cover the content. Potential loss of millions of dollars is to value of an amount. Strategy to reduce risk and immediate actions Should include risk, staffing, software and hardware requirements, timelines, and staff training needs. Additional security testing may be a regulatory requirement which may be required to be done even if they don't want to do it. State work completed by all team members even those not present.

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	250	125	0	0	0

Whack a Mole		
WAM1	WAM2	WAM3
125	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
1360	0

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)
16	23	26	27	19	27	27	27	27	27	26

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
0.00	0.00%

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
1340

Green Team Survey Comments

- Pay attention to your navigation bar and users! also, the oil rig status page isn't operational.
- "Site looks good, but I had no access to the 'Admin Dashboard'. I could log in and there was no 'Admin' button, but it only returned me to the main screen.
- users not populated in user management page. no footer included in homepage.
- user management was there but the one user was not an admin. The career section did not have the careers. Site color was a little light.
- company name misspelled, blue admin and green admin not showing on user management page, footer not visible on main page
- Colors seem a little 'Red' rather than Maroon. Yep they are definitely RED! Looks like red user added and promoted to admin. No Career Positions, but good benefits :) No footer on Home Page. Graphics slow loading, maybe DOS attack underway. But Rig Status is valid :)
- More accounts have admin privilege. Footer text and Title are missing 'Rift' for the company name.
- Looks like you have a Jason Bourne admin users :-D Oh, and Red admin user, that's not good.
- Good job
- Great Job!