



UNITED STATES AIR FORCE ACADEMY

DELOGRAND

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 39 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	645	43.00%	16
Security Documentation	1125	90.00%	27
C-Suite Panel	968	77.44%	57
Red Team	1125	45.00%	35
Blue Team	1813	90.65%	37
Green Team Surveys	1200	80.00%	34
Deductions	0		
Overall	6876	68.76%	34

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 | 645

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

1	Yes
2	Yes
3	No
4	Yes
5	Yes
6	Yes
7	No
8	
9	No
10.1	Yes
10.2	Yes
10.3	No
10.4	Yes
10.5	
10.6	

10.7	
10.8	
10.9	
11.1	Yes
11.2	Yes
11.3	Yes
11.4	Yes
11.5	Yes
11.6	
11.7	Yes
12	
13	
14	
15	Yes
16	Yes

17	Yes
18	Yes
19	Yes
20	Yes
21	Yes
22	
23	
24	
25	
26	
27.1	No
27.2	No
28	Yes
29	
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 | 1125

Strong Points	Areas of Improvement
<ul style="list-style-type: none">Good list of vulnerabilities and hardening.The team provided comprehensive coverage of vulnerabilities across systems and offered meaningful mitigations. Their hardening steps are practical and well aligned with best practices. The document's structure is clean, organized, and professional.The document looked professional.Covered great amount of details with clarity and looking good to present. Overall great effort by the team.	<ul style="list-style-type: none">The overview needed some work to include all systems.Several vulnerabilities are written too generally and should include root causes and technical details explaining why they exist.Informational notes that do not represent real risks could be removed or placed in an appendix.It would be beneficial to add CVE identifiers or severity classifications for consistency.Finally, including a brief summary of the potential business impact of each major

Strong Points	Areas of Improvement
	<p>vulnerability would strengthen the leadership value of the report.</p> <ul style="list-style-type: none"> Minimal justification was given for hardening steps. The hardening section can be formatted little better to keep some spaces instead of looking too bulky.

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 | 968

Strong Points	Areas of Improvement
<ul style="list-style-type: none"> The professionalism of this team is exemplar. I feel like I have been in business meetings much like this one. Each member of this team is dressed immaculately and the slide deck is clean and professional. Furthermore, the dissolve from one speaker to the next is a fantastic way to conserve our valuable time while allowing us to flow from one speaker to the next. This team truly set the bar when it came to the look of how a talk to executives should look. Truly well done! Very professionally dressed and the presentation was well done, except the video itself - hard to hear the presenters and very hard to read your slides. Brownie points for highlighting supply chain risk. I really liked that multiple folks presented on different topics within the presentation. It would have been nice to know if this was the entire team and what their contributions were to the presentation or competition effort. I also liked the Cost Benefit Analysis that was presented. I thought the risk section was well done, especially including risk of no action. Directly addressed aforementioned risks. The presentation was professional and well reasoned out. 	<ul style="list-style-type: none"> The biggest miss for me in this presentation is that the only thing that is discussed at all in terms of cost are the High Priority Recommendations, which are "Free" or "no additional cost." From everything that I have learned in cybersecurity, executives need clear data especially overtly laid out data in financial terms. How did this incident impact our bottom line? Every other presentation I've seen so far at least gave me the stat of \$124,000 per day in lost oil revenue, and many extrapolated the associate costs much further. Even the Summary – Cost Benefit Analysis slide didn't offer a single, actual cost, instead speaking in abstracts. Execs need cold hard facts, especially financial ones, not platitudes. Next time you speak to leadership (which I am certain that each of these young professionals will be doing in their near futures), come armed with actual numbers. It was impossible to read the content of the slides. I did find the volume a bit low, but closed captioning took care of that for me. For some slides there was a glare in the room, making the slide difficult to read. Overall great effort! Your risks could have been more thoroughly tied to the bottom line. Don't just tell us they affect the bottom line. For example, tell me how risks to personnel safety affect our operations and business functions.

Strong Points	Areas of Improvement
	<ul style="list-style-type: none"> It was a bit hard to see the slides, but overall it was a good presentation

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	250	0	0	0	0

Whack a Mole		
WAM1	WAM2	WAM3
250	125	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
1445	368

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	24	27	22	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
32223.68	71.61%

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
1200

Green Team Survey Comments

- footer is incorrect – says 'http://blue.local'
- Red team has admin tag
- The homepage does not have a footer.
- cannot login as user or admin
- Great job, good luck!
- Unable to reach the website.
- 504 Gateway Time-out
- Hello Team 39 I was unable to log into admin middleware.
- Webpage would not load. Error message: web.blue0039.cfc.local refused to connect.
- Received a 502 Bad Gateway message when trying to pull up the site. :-(
- all good