



THE UNIVERSITY OF TULSA

GOLDEN DRILLERS

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 45 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	480	32.00%	37
Security Documentation	1177	94.16%	18
C-Suite Panel	919	73.52%	69
Red Team	750	30.00%	53
Blue Team	1782	89.10%	40
Green Team Surveys	1397	93.13%	46
Deductions	0		
Overall	6505	65.05%	46

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	480
----------------------	------------

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	No	19	Yes
4	Yes	11.1	Yes	20	No
5	Yes	11.2	Yes	21	Yes
6		11.3	Yes	22	
7		11.4	Yes	23	
8	No	11.5	Yes	24	No
9		11.6		25	
10.1	Yes	11.7	Yes	26	
10.2	Yes	12		27.1	No
10.3	Yes	13		27.2	No
10.4	Yes	14		28	
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	1177
-------------------------------------	-------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> Network diagram is clear and informative This team effort was really thorough and well done. The things that really stood out were the network diagram showing all the logical connections and a useful legend. This is one of the best network diagrams that I have seen. The asset inventory detailed all the ports and protocols explicitly and concisely. All of these components would be appreciated by senior management when presenting the report and the way they are organized really helps with readability. One more thing that stood 	<ul style="list-style-type: none"> Differentiate between mitigation of vulnerabilities and hardening of the system overall with justification for each hardening step. Consolidate CVEs when possible. Overall this is an excellent submission, so there are only a couple areas that could add improvement. First is to simply remove any of the template language, especially instructions to the team that is usually in italics, senior management doesn't need to see this in the presentation, but that is a small thing. A couple other suggestions would be; add a few more sentences to the

<i>Strong Points</i>	<i>Areas of Improvement</i>
<p>out is the System Hardening section, the narrative description provides an excellent walk through of the vulnerabilities discovered on each component and then the decisions made on tools to use and mitigations that were applied.</p> <ul style="list-style-type: none"> • The system overview was very well written and explained each system in laymen's terms enabling the c-suite to follow critical information. • amazing job with the network diagram 	<p>System Overview that specifically describe areas of focus or concern as a "bottom line up front" type of description to the senior management, such that if they only read that first paragraph they will have an idea of overall scope and the imminent issues. And then finally, in the System Hardening section, which again has an excellent narrative description, it might be helpful in presentation form to include a small bulleted list or table under each paragraph that shows for example on the AD component - issues identified, mitigation/fix, tools used. This could improve readability for senior management.</p> <ul style="list-style-type: none"> • Asset inventory: AD missing port 38. Mark hosts where breaches are being assumed. In the system hardening, think of ways to visually split up the information whether that be through headers or other formatting options to help the reader jump between sections depending on what information they are looking for. • structure your system hardening responses into sections

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	919
----------------------------	------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> • Holistically, I believe that your team offered a professional and engaging presentation for leadership. This presentation was clearly well researched and there was a lot of thought about the overarching incident and potential remediation options. Furthermore, the slide deck was clean and each slide and person flowed organically from one to the next. • I enjoyed all the team members participating in the presentation. • The strategies to reduce business risk didn't directly relate to identified risks • Good work on listing sources. • Good slide design and use of video embedded over slides. 	<ul style="list-style-type: none"> • I love that right from the start that Aiden highlighted risk in terms of financial terms. This four million dollar figure was startling and caught our attention. The problem was that this was the only mention of any figures at all. Just on this slide, what is the potential cost for damage to infrastructure or the cost of reputation? And what about the Complete Risk Reduction Strategy where the first recommendation was to Appoint an on-site network specialist—employees cost money and specialist employees cost a lot of money. Contrast this with High-Priority Actions where Nmap is a free tool (although you need someone familiar with the technology to use it well as Nmap is typically

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> • good team work, good coverage on strategy to reduce & recommendations. also stating the cost for the 33 day outage at \$4M+ vs \$120K a day will get the C-Suites attention better. • Excellent video, well rounded analysis without technical jargon is exactly what the C-suite wants! 	<p>used for actively probing networks to learn something like vulnerable open ports rather than an intrusion detection system or intrusion prevention system that would reflexively allow users to channel resources to threats against the system). As a presenter, your job is to make it as easy as possible for your audience to follow your insights and recommendations—and cache all of these in financial terms so that your audience truly understands the cost/benefit analysis at work here.</p> <ul style="list-style-type: none"> • Slides were basic, and the presentation was not rehearsed. One presenter was reading the script way too fast. • The information was presented well. Including your sources is an excellent practice. • The title of the sources should also be included • Complete Risk Reduction Strategy should be quantified, time and cost. • Network mapping should then be followed by vulnerability scanning and remediation. • More detailed needed, how will security and access control be strengthened • Immediate and future benefits, seems to list the same contents as the previous slides without adding future context. This slide could be removed and further details and context could be added to previous slides. • A single on-site specialist may not be able to handle the scope and depth of the regular work, and would then be limited in the ability to remediate an active threat and incident • Risks related to Business & Operational only had the outage cost vs reputation, federal compliance, injury considering OT etc. Prior recommendations were comprehensive but didn't discuss cost, even if intimated low cost. • I would have liked to see more about IT/OT segmentation or details on how to better isolate the OT risk as a high priority

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	0	0	125	0	0

Whack a Mole		
WAM1	WAM2	WAM3
250	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
1390	392

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)
25	22	22	26	27	25	27	25	26	26	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
34258.45	76.13%

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

1397

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

- The footer needs to be lower on the home page, but no mistakes.
- When logged in the site did not have an admin button as per instructions.
- Red team has admin tag
- Fix the footer and background photo size
- red user added
- There is no footer on a home page
- Good job
- No footer on Login or Sign Up. Nice work otherwise!
- Maroon tint needs fixed, only covers part of image
- Great job
- Rock-solid work! Even Obsidian Rifts rigs approve” Unfortunately, you’re missing the footer on the login and signup pages.
- Good job! Your tag line is at the top of the page rather than in the middle of the image. The accent color is not covering the full graphic image as it should we you first open the website. You have all the proper admin users, but there is a red admin user within the portal!
- This site cant be reached web.blue0045.cfc.local refused to connect.