



JOHNS HOPKINS UNIVERSITY

JHU

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 55 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	442	29.47%	44
Security Documentation	1178	94.24%	16
C-Suite Panel	1000	80.00%	48
Red Team	750	30.00%	53
Blue Team	1820	91.00%	35
Green Team Surveys	1412	94.13%	43
Deductions	0		
Overall	6602	66.02%	43

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	442
----------------------	------------

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		11.1	Yes	20	Yes
5		11.2	Yes	21	
6		11.3	Yes	22	
7	Yes	11.4	Yes	23	
8	No	11.5	Yes	24	
9	No	11.6	No	25	
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	

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	1178
-------------------------------------	-------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> Overall, good documentation. System overview was detailed and sets the documentation up on the right foot. Asset inventory and network diagram are both solid entries. This report demonstrates outstanding performance, meeting or exceeding expectations in all key areas. The team successfully tailored the system overview for a senior leadership audience, provided a complete and precise asset inventory listing all six VMs with specific details, and delivered a logically coherent network 	<ul style="list-style-type: none"> Avoid using jargon on senior leadership; they might not know what you are talking about. More even distribution of attention on vulnerability identification on the systems (none were listed for PLC) would be beneficial as to not miss out on even coverage. May be beneficial to re-structure system hardening to be a broader overview that directly matches the procedure you listed / potentially align it to a framework or CIS benchmarks. A clear plain-language

<i>Strong Points</i>	<i>Areas of Improvement</i>
<p>diagram that included all required components. Furthermore, the vulnerabilities section was exemplary, documenting far more than 30 unique issues with appropriate mitigations, all presented in a professional format that avoided raw scanner reports.</p> <ul style="list-style-type: none"> The diagram is easy to read, and has a key. Very good detail on your vulnerability mitigations. 	<p>explanation for each step taken would assist executive audiences.</p> <ul style="list-style-type: none"> fix typos and standardize terminology for professionalism; align domain naming with competition guidance (e.g., use "cfc.local"); correct the asset inventory by listing host-based controls like "Windows Defender Firewall" as part of a host, not as a separate asset; enhance the network diagram by adding logical data-flow connections (e.g., Webserver to DB) instead of just physical links; and clearly label "assume breach" recommendations as non-actionable constraints to avoid confusing leadership. In the System Overview, what does the system itself do? What is the sum of its parts? Good system hardening steps, but would like to see more justifications.

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	1000
----------------------------	------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> I like that you had environmental liability. That was not a common answer but should have been. Risk well presented and valuable. Everything was done well. The presentation looked professional. Well designed slides. Good work on embedded video over slides. Good work referencing NIST Your risks were exhaustive and clearly related to business functions. 	<ul style="list-style-type: none"> Presenters should introduce themselves when first talking. Audio levels between speakers were not consistent. The Key Priorities presenter was just reading the slide. Strategy and recommendations were too general and difficult to relate to the risks presented. Some of the slides were a little busy and had too much information. Some slides are quite wordy. Recommend including costs, timelines, equipment, software, and staff requirements for response strategy, and recommendations. Recommend including a references slide. Its good form to orally tote your team ID and introduce your team members by name. Also, make sure audio is consistent across all speakers. Finally, make sure your risk reduction strategies directly address your aforementioned 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	0	0	0	0	125

Whack a Mole		
WAM1	WAM2	WAM3
125	125	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	345

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
30156.64	67.01%

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

1412

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

- | |
|---|
| <ul style="list-style-type: none">• Footer text read 1841 Convention Center Dr instead of 18451 Convention Center Dr• red team has admin• check your footer and admins!• red user added• good job• Good job• Great job! You secured that oil rig so tight even the crude couldn't slip past you!• Perfect website!!!• Perfect!• Good job! You have all the appropriate admin users, but there is a red user that has made its way into the admin directory. Your rig status is also 'Normal Operation'.• site cannot be reached |
|---|