



PURDUE UNIVERSITY NORTHWEST

PNW CYBER ROAR

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 67 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	285	19.00%	77
Security Documentation	1128	90.24%	26
C-Suite Panel	1039	83.12%	37
Red Team	1375	55.00%	22
Blue Team	1475	73.75%	68
Green Team Surveys	1309	87.27%	41
Deductions	0		
Overall	6611	66.11%	41

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	285
----------------------	------------

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

1	Yes	10.7	Yes	17	No
2		10.8	Yes	18	Yes
3		10.9		19	Yes
4		11.1	Yes	20	No
5	Yes	11.2	Yes	21	
6		11.3	Yes	22	
7		11.4		23	
8		11.5		24	No
9		11.6		25	
10.1	Yes	11.7		26	
10.2	Yes	12	No	27.1	No
10.3	Yes	13		27.2	No
10.4		14		28	No
10.5	Yes	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	1128
-------------------------------------	-------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> good inventory and network diagram. Team 67 shows very strong technical coverage and execution, with a complete asset inventory, clear network diagram, and detailed hardening steps grounded in standard tools and best practices. The hardening section stands out for its depth and excellent explanation of the steps, tools, and logic behind each security improvement. Overall was a good document and it was great seeing the clear separation between machines in the middle three sections. 	<ul style="list-style-type: none"> For the overview, I would have liked less technical jargon and more vulnerabilities needed to be listed. It relies heavily on technical detail and notation that are not suited for senior leadership. The overall number of vulnerabilities is high, but it lacks ICS mitigations. Some of the vulnerability descriptions could be shortened or grouped by system type to make the section easier to scan without losing important details.

<i>Strong Points</i>	<i>Areas of Improvement</i>
	<ul style="list-style-type: none"> • More justification is needed for the hardening steps that were taken.

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	1039
----------------------------	-------------

<i>Strong Points</i>	<i>Areas of Improvement</i>
<ul style="list-style-type: none"> • I like that you showed the impact of a similar attack. • Risks and strategy well presented, strong explanation • Broad strategies to manage strategic risk • Excellent job describing risks. You give actual cost estimates, and don't dwell on the current incident, but rather on the risks related to the current security posture • Well-done presentation with clear organization and thoughtful delivery. The team demonstrated good understanding of the material and maintained strong focus on the key objectives. • Included business risks for operational security on an executive level (i.e. stock pricing and insurance claims). Nice transition from high priority recommendations to future risks. 	<ul style="list-style-type: none"> • what about environmental risks? Match your strategies to your risks. • Missed a long term strategy well and clearly explained. Dress could be more professional and time could've been used better not expending too much time on future risks. • Tie strategies and recommendations to incident risks • The strategies you outline are actually high priority recommendations. Strategy should be longer term thinking and higher level such as: Modernize the cybersecurity training program and integrate into institutional training program. THEN you tie that strategy to how it will reduce the risks you identified. On the flip side, your high priority recommendations could almost be a strategy. Overhauling network architecture is not something to be taken in the short term; it is more strategic. For high priority recommendations, provide an estimate of cost. • You're progressing well — continue building confidence in your delivery and look for small ways to add depth or real-world connection to strengthen your overall professional presence. • Elaborate more on specific free or open-source tools that might be used. If you can refer to the ICS compromise and explain how your strategy would secure the offshore platform.

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	125	250	0	0	0	125

Whack a Mole		
WAM1	WAM2	WAM3
125	250	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
1475	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)
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
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

1309

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

- Footer is visible on every page except the homepage
- No footer on the home page.
- No footer on the home page
- footer text not visible on main page
- Address footer is supposed to be on every web page, but it's not found on the home.
- footer not available in main page
- No footer on Home Page.
- No footer on home page, Login, or Sign Up. Nice work otherwise!
- Recommend putting the footer on the home page too like it is on the others.
- you have no footer on the front page.
- Blue learn more button, No footer on homepage
- Footer not on all pages
- 5:44 This site can't be reached
- This site can't be reachedweb.blue0067.cfc.local refused to connect.