WESTERN WASHINGTON UNIVERSITY

VI_KINGS

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 95 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	413	27.53%	52
Security Documentation	981	78.48%	63
C-Suite Panel	1048	83.84%	32
Red Team	750	30.00%	53
Blue Team	1803	90.15%	38
Green Team Surveys	1206	80.40%	55
Deductions	0		
Overall	6201	62.01%	55

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	413

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	Yes	19	Yes
4		11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6		11.3	Yes	22	
7	No	11.4		23	
8	No	11.5	Yes	24	
9	No	11.6		25	
10.1	Yes	11.7		26	
10.2	Yes	12	No	27.1	
10.3	Yes	13	Yes	27.2	
10.4	Yes	14		28	Yes
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	981

Strong Points	Areas of Improvement
• Presents a well-rounded, technically strong package, clear system description, complete asset inventory, and excellent diagram. • I like the network graphic diagram and detail documentation • Asset table was easy to read, don't be afraid to take up space though and give each item it's own line. • The overall presentation. • Appreciated the complete asset inventory and the amount of vulnerabilities found.	• Have some minor typos, and could've enumerate host-specific control sets(like password policies). • Formatting in system hardening made it difficult to read. Use of paragraph spacing or indentation and lists would have improved this section. • Analytical skills could be stronger and more attention, particularly when it comes to data interpretation. • System hardening steps need to be more elaborated and thought out for the overall impact of the systems.

Strong Points	Areas of Improvement
• good analysis of issues and mitigation strategy. Network diagram was well made and easy to understand.	• A deeper analysis would help identify more issues and mitigation strategies, seems like you might have missed some issues. Some editing of the writing would give audience more clarity. Please make sure you delete template instructions as it distracts from your end product.

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	1048

Strong Points	Areas of Improvement
• Efficient use of time. • Team 95 delivered an exemplary C-Suite briefing, excelling across all content-focused categories, risk analysis, strategy, and high-priority recommendations. They clearly articulated operational and business risks, including contractor sourcing and safety concerns, and quantified financial impacts at approximately $125,000 per hour during unplanned shutdowns. Their strategy was comprehensive, featuring multiple long-term actions such as continuous monitoring, access management, and data classification policies. High-priority recommendations stood out for fully meeting funding constraints by using free software for firewall/IDS solutions, with well-reasoned links to mitigating identified risks, demonstrating strong alignment with task requirements and C-Suite expectations. • Nice summary of risk strategy • Covered and outlined business risks and operational impact following an industrial control system compromise, with direct ties to reputation, safety, and production. • The justification for your high-priority recommendations was great.	• Risks were mainly business related, strategy not fully related to the risk to be able to understand the strategy. • Presentation Time, Required Elements (2% Weight): Although the team named all members (Clay, Alex, Ella, Nick, Maksim, and Quinn) and had two active presenters, they fell short of the Exemplary requirement for acknowledgment. To achieve the highest score, the team needed to provide a ""Clear acknowledgment of contributions from all (either on- or off-screen) team members"". Next time, state the specific roles or contributions of the non-presenting members (e.g., "Nick handled the risk analysis,"" or ""Ella developed the DRP outline""). • Quality of Presentation (8% Weight): While the team used slides, the presentation reportedly lacked visual charts and calculations. Visual aids, slides, and other materials must have a consistent, professional appearance to earn an Exemplary score. Including professional visuals such as charts displaying the estimated financial impact (e.g., the $125,000/hour loss) or graphs illustrating the timeline and cost of the three high-priority recommendations would have significantly enhanced the clarity and professionalism of the briefing for the non-technical C-Suite audience. • Better understanding of future risks

Strong Points	Areas of Improvement
	• Recommendations could be more quantified (financial analysis of prevention costs versus risks) and tailored to Obsidian Rift Energy's specific environment. Vendor management and risks could be more specific. • Possibly on the fast side.

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	250	0	250	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
1475	328

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
28679.97	63.73%

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
1206

Green Team Survey Comments

- logos not in right place, but there. Blue Admin and Green User got deleted
- Admin user do not show up
- Under Admin, the user list is incomplete. The homepage does not have a footer. The is a logo but did not follow the required location.
- Blue and green admin user is missing and recommend having the footer on the home page and suggest repositioning your logos as the positions don't match the initial setup where logo on each side of company name.
- Missing admins, no footer on main page
- No admins listed, no footer on main page
- footer text not found on homepage. admin users not found.
- Footer missing from main page
- no admins listed, no footer on main page
- Blue and green admins missing from admin page
- green and blue admin not available on user management, main page doesn't have footer. logos not surrounding company name
- green and blue admin missing from user management, footer missing from main page
- green and blue admin not in user management, footer missing on main page
- This site can't be reachedweb.blue0095.cfc.local refused to connect.
- 502 Bad Gateway nginx/1.19.0"