



VIRGINIA TECH

PWM@VT

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 69 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	267	17.80%	81
Security Documentation	789	63.12%	84
C-Suite Panel	927	74.16%	66
Red Team	0	0.00%	91
Blue Team	1723	86.15%	49
Green Team Surveys	448	29.87%	83
Deductions	0		
Overall	4154	41.54%	83

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 | 267

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

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

10.7	
10.8	
10.9	
11.1	
11.2	
11.3	
11.4	
11.5	
11.6	
11.7	
12	
13	No
14	
15	Yes
16	Yes

17	Yes
18	Yes
19	Yes
20	Yes
21	
22	
23	
24	
25	
26	
27.1	No
27.2	
28	No
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 | 789

Strong Points	Areas of Improvement
<ul style="list-style-type: none">Good job defining acronyms before using the shortened version.The system overview was well written and went from a macro view to a system view.This report contained solid content and demonstrated a high level of technical skills.Overall good beginning documentation. The network diagram had a surprising amount of information.The document is well written, demonstrating careful thought and attention to structure. The network	<ul style="list-style-type: none">While it is acceptable for the diagram to be handwritten, it was hard to read some text in it due to small handwriting.The system overview and system hardening sections could target a 'senior leadership' audience better.Some inaccuracies in the asset inventory, such as using the wrong IP for the task box and not describing the service of the ports in a few places (e.g., listing port 139/445 for SMB on the task box rather than 'Intended to be used by blue team to fix the system').

Strong Points	Areas of Improvement
diagram adds clarity to the overall picture, and the recommended mitigations are realistic and actionable.	<ul style="list-style-type: none"> Some issues with smaller formatting details. For instance, there were extra rows from the asset inventory table that took up an entire page of the document. Another example was using italics in the first row of the asset inventory table. More justifications in hardening section were needed. I really recommend checking out different diagramming programs. DrawIO is free and will allow you to create network maps. The template wasn't removed, the report read like notes, not a report, sometimes the formatting made it hard to read. Double check that the network diagram and asset inventory are conveying the same information. Some vulnerabilities are labeled as "resolved," but the mitigation text still reads as "planned," and these should be updated for consistency. Severity or prioritization levels should be added for each issue to help focus efforts. IP assignments should be reviewed to confirm accuracy between the asset list and findings. Finally, a short description of the potential business or operational impact of each vulnerability would add context for making decisions.

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	927
----------------------------	-----

Strong Points	Areas of Improvement
<ul style="list-style-type: none"> Overall, I think that this team did a very solid job with the rhetorical moves here. The slide that most impressed me was the one on Risks and Impact where the threats were cached in millions and billions of dollars and even more important loss of life. And all of this was complimented by the graphic image of the Deepwater Horizon in flames. Similarly, the Immediate Actions offers a clear and succinct plan for what to do and when. This team is exception in getting us 	<ul style="list-style-type: none"> My concerns here are the actual recommendations. While disconnecting remote connections is a brilliant first step and ongoing cybersecurity training for staff is great for mitigating future issues, neither of these are going to solve the overarching issue. Once isolated, do you wipe all the system and reinstall everything? Do we have such backup and if we do can we afford to be offline for those days, weeks, or months? And while Wireshark is great and free, this tool simply captures packets.

Strong Points	Areas of Improvement
<ul style="list-style-type: none"> feeling the gravity of this situation and offering clear guidance on how to get out. The team summarized the risks and how they affect the company's concerns and finances in a manner that would be understood by any C-suite executive. The risk management plan details risks, appropriate mitigations, and subsequent actions with comments on tools that could be used and the potential costs (or lack thereof) of those tools. The high priority actions were laid out well with this teams version of immediate and long term ranging from hours up to 14 days in the timeline. For the risks, I really liked how you gave the Deepwater Horizon Oil spill as a baseline for how much these incidents can cost. Your Immediate actions are excellent, but remember to give a cost estimate and avoid jargon (lateral movement) The team provided strong reasoning for priority recommendations including timelines. The risks were decently explained 	<p>While more data is great, we need something that can parse out this data and identify what is concerning and what is normal operations. And you mention deploying the CSIRT to gather forensics: Do we have this team on staff or are you suggesting that we hire a third-party here? And how much will either of these cost us? And what is the value of forensics? Does it directly impact our first priority Business Continuity and Disaster Recovery? We have to focus on weathering the event and doing all we can to get back to a semblance of normal before we can have the luxury of understanding what happened.</p> <ul style="list-style-type: none"> It would have been nice to see other recommendations that would support the cybersecurity posture of the organization with a plan that could be enacted ranging from months to up to a year. The risk management plan has some references to techniques that are applicable for the long term but that isn't specifically noted. I like your approach for risk mitigation in that the actions tie directly back to your ICS risk, but you haven't talked about an overall longer term strategy to take. Also, remember that training is not free. Even if the content is free, the time it takes staff to take the training in addition to the overhead of providing and tracking it is quite expensive. Strategy to reduce risks did not focus on the long term and seemed to be more tactical and focused on the now. Justifications needed more depth in general

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	0	0	0	0	0	0

Whack a Mole		
WAM1	WAM2	WAM3
0	0	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
1270	453

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)
21	27	25	25	21	19	27	8	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
39618.82	88.04%

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
448

Green Team Survey Comments

- check your careers, headers and footers, make sure things like login are operational!

Green Team Survey Comments

- Your web server appears to be compromised.
- Logos in header too small, Address is wrong, no login just sign up button, careers not on page and site color is yellow.
- "Site is color is Green No open position on careers page no footer address on home-screen no login button"
- "The color is yellow. No Login option menu. The tagline says opposite than the what it supposed to say. No career options. The company name and the address are incorrect in the footer. The logo location is incorrect."
- company name misspelled, no login button, footer not right
- accent color is gold/goldenrod. No background picture. Tagline reads 'Spilling Oil is Good. Spilling Data is Better.' Nav bar is missing login button. Company name is incorrect. No position listed on Careers page. footer info is incomplete, no street address or city.
- header color yellow, company name misspelled , no login, careers all gone
- logos too small
- your colors are off, and so is your navigation bar and logos. Your homepage tagline is wrong, and your homepage has no footer. Your careers are gone, and logging in is not an option. Your footer on other sites are not accurate.
- Colors are wrong, company name is wrong, logo in wrong spot, tag line text wrong, and no login button
- "Logos not correctly placed color scheme [yellow] headline reads 'Spilling Oil is Good. Spilling Data is Better.' [lol] footer missing login option missing [cannot verify]"
- Website does not load.
- website down
- 5:44 This site can't be reached