U.S. DEPARTMENT OF ENERGY'S
CYBERFORCE COMPETITION®
DEFENDING U.S. ENERGY INFRASTRUCTURE

THE UNIVERSITY OF RHODE ISLAND

RHO-DAY

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 72 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	330	22.00%	70
Security Documentation	785	62.80%	85
C-Suite Panel	966	77.28%	59
Red Team	500	20.00%	70
Blue Team	1475	73.75%	68
Green Team Surveys	1357	90.47%	71
Deductions	0		
Overall	**5413**	**54.13%**	**71**

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	330

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		10.9		19	Yes
4		11.1	Yes	20	No
5	Yes	11.2	Yes	21	
6		11.3	Yes	22	
7	No	11.4	No	23	
8		11.5	No	24	No
9		11.6		25	
10.1	Yes	11.7		26	
10.2	Yes	12		27.1	No
10.3	Yes	13		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	785

Strong Points	*Areas of Improvement*
• Strong documentation and analysis. • In this report, the content was solid, and a high level of technical skill was demonstrated. • Great job overall and well done on ensuring that there was proper justification for each hardening step. • Rotating the blueteam passwords is a good idea, even though it's likely that that account is on a red-team no-strike list.	• Missing known vulnerabilities, the red team planted many more than what was listed. • The template wasn't removed, formatting could have made the report more readable, the report was not always appropriate for c suite. • Expand on the network diagram more to ensure that all logical connectors are in place. • Requiring 12-character passwords which have to be changed every 30 days is likely to frustrate users and encourage other poor password use policies. Blindly applying

Strong Points	Areas of Improvement
	patches on a PLC or HMI system is likely to cause substantial, unexpected downtime.

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	966

Strong Points	Areas of Improvement
• Slides are well done. 5 pillars - only team to use this. • Nice job, easy to follow and at the right level for the C-suite. • I like the font of the presentation and able to identify the risk and come up with solution • Comprehensive Risk Analysis: The presentation provided a clear summary of business and operational risks posed by the ICS compromise, which included the escalation from minor irregularities to a 40-second blackout and an over-pressure condition. Team 72 clearly identified how these risks affect the company's bottom line (finances) by detailing the financial impact of downtime, the need for investment in repair and remediation, and the exposure to insurance/liability claims due to equipment malfunctions and safety hazards. This presentation was appropriate for the C-Suite audience, avoiding a technical walk-through of vulnerable network assets. • Complete Risk Reduction Strategy: The team provided a complete strategy to reduce risk that included five key pillars (Segment and Control Access; Standardize and Maintain; Detection and Incident Response; Backup Restoration and Continuity; Governance and Oversight). This approach surpasses the requirement for an Exemplary rating, which mandates ""three or more long-term action items and/or policy updates,"" and the strategy clearly addressed the previously identified risks. • Effective Prioritization: The team provided three high-priority recommendations (Quarantine and Lockdown; Monitoring and Detection; Communication and Training)	• Thank you slide - convert to Questions. You work for the C-Suite, they will have questions for you. This will not be a fun in-person meeting. Do not put paragraphs on slides, use bullet points instead (Cause and Scope slide). No timeline provided. No impact to company finances. No names of apps to be used given. No cost of strategy to reduce risks - C-Suite is about the bottom line ($$$). Asking for a 14-day shutdown without a strong case to back it up ignores the cost to the company and will likely be rejected. • I didn't hold it against you in scoring, but I feel it's worth pointing out the Activate Windows watermark in your presentation. Even with a valid reason, when presenting to non-technical stakeholders, optics matter. Some may see that and think nothing of it but it could be a red flag for others. It would be fair for executives to question your work. Is it a lapse in system hygiene? Do they have confidential business sensitive info on a machine outside IT control? If my own cyber team is using a misconfigured device for an executive briefing, where else are they sloppy? Again, you may have a valid reason, but executives expect their experts to model operational discipline in their field. SME's help set the tone for the acceptable culture for everyone else. • Needs to mention the financial impact of the company • Improve Professionalism in Visual Aids (Quality of Presentation): The presentation materials lacked a consistent, professional appearance. The use of slides that are a bit wordy and lacking ""graphs and

Strong Points	Areas of Improvement
that provided complete and consistent reasoning aimed at stabilizing the system quickly. • Well designed slide and graphics • Very good overview of the incident, but you spend too much time on it. I like your strategies and how they are categorized.	calculations"" suggests the visual aids were insufficient for a high-level briefing. Future submissions should aim to use professional visual aids that summarize data concisely for the C-Suite. • Ensure High-Quality Audio (Presentation Time, Required Elements): Attention must be paid to the technical quality of the video. The observation that ""the other team member microphone wasn't loud enough"" constitutes an audio distraction, making parts of the presentation difficult to follow. All participants must be heard clearly and equally. • Adhere to Funding Constraints for High Priority Recommendations: While the recommendations were strong and well-reasoned, achieving an Exemplary score requires that high-priority actions utilize only free or open-source tools and require at most a minimal level of additional funding. The team requested funding for logging enablement and backup validation. To achieve the highest score in this category, future recommendations should clearly articulate how proposed actions can be completed using free/open-source tools while addressing the limited/non-existent funding constraints. • Should discuss the roles of the other team members. • Zoom recording settings are incorrect. The Zoom menu bar should not be visible at the top • Jargon on slides. Terms should be explained for C-suite non experts • Business impact should be quantified, financially, downtime estimates, etc. • Strategy slide is too wordy. Should include discussion of staffing, costs, timelines, hardware and software needed, etc. • High priority recommendations completed within the next few days is a very short and unrealistic timeline. • Should end asking if the viewer has any questions, and with a list of references. • Strategies are good, BUT it isn't clear how they reduce the risks you just got done articulating. If safety is a risk, then which

Strong Points	*Areas of Improvement*
	part of your strategy to reduce risk improves safety?

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	125	0	0	0

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	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
1357

Green Team Survey Comments
• No footer on the home page
• Excellent work!
• "No footer on the main homepage. I did not deduct the point but the User Management page didn't have 'green-user@obsidianrift.oil' as a user though 2 admin users were listed."
• no footer on a home page
• footer not available on main page, green user missing
• footer not available on main page, green user deleted
• No footer on a Home page,
• Could not scroll to the bottom of the homepage to validate the text. Good luck!
• Footer missing from main page
• you do not have a footer on the front page. Otherwise, good job!
• The footer text is missing from the main page -- I've tried resizing the window and am unable to view footer for main page as the template indicates.
• Recommend putting the footer on the home page like the others.
• website is down