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

OREGON STATE UNIVERSITY

DAMSEC (FORMERLY OSUSEC)

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 36 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	528	35.20%	27
Security Documentation	1187	94.96%	14
C-Suite Panel	1123	89.84%	9
Red Team	1125	45.00%	35
Blue Team	1477	73.85%	67
Green Team Surveys	1227	81.80%	36
Deductions	0		
Overall	**6667**	**66.67%**	**36**

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	528

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

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

10.7	Yes
10.8	Yes
10.9	Yes
11.1	Yes
11.2	Yes
11.3	Yes
11.4	Yes
11.5	Yes
11.6	
11.7	
12	
13	
14	
15	Yes
16	Yes

17	Yes
18	Yes
19	Yes
20	Yes
21	
22	
23	
24	
25	
26	
27.1	Yes
27.2	Yes
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	1187

Strong Points	*Areas of Improvement*
• Good list of vulnerabilities and hardening approach. • The documentation was thorough and complete. • Very professional doc. • Your hardening techniques were very thorough and clearly reflected real technical understanding. The depth you provided shows strong potential for professional-level documentation and defensive operations work.	• The network diagram needed some work. • The system overview is unclear. • Summary a bit minimal. • You delivered a strong and technically solid presentation. The only small improvement would be simplifying a few phrases so the message connects even more clearly with a C-suite audience. Your work shows real skill and solid understanding, and you should feel confident about the direction you're heading.

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	1123

Strong Points	*Areas of Improvement*
• Very professional, 1st speaker was full of energy, gave impression of competence. Only team to mention baselining. Revising contractor policies was mentioned by 1/3 of teams. • Speakers were well-rehearsed and slides well-organized. The risk section was particularly effective in splitting overall risk into three subsections and analyzing them there. • In-depth technical explanation of the points presented especially in the Risk section. They did a great job in all areas in my opinion • Felt like you did a very good job of selling me on the risks to the business, really got me thinking about all the areas this cyber attack can impact the company. • Risks were excellently detailed and well thought out. Like how you had relevant regulations identified. • Well designed slides. Good use of video embedded over slides.	• Label speaker with names under their video. 2nd speaker should move camera to show them face on. Lots of time spent on rig personnel safety - this was not the issue. No slides showing timelines of recommendations or costs. This is what the C-Suite focuses on! • Quantifying the risks helps the c-suite understand the importance of taking action. For instance, discussing exactly how much money the loss of oil could cost per day or regulatory fines from environmental harm or lawsuits over personnel injury would be helpful to the presentation's effectiveness. • They could explain what are the regulations listed and how it is pertinent to the slide deck. Like EPA: 40 CFR 55 • I like the recommendations but try to stay in the cyber lane, my initial thoughts when you suggested notifying regulators was "what does this have to do with cyber", unless there is something very specific to cyber & regs I need to be aware of, this slot is better used for other cyber recommendations. For an org like this, the C-suite has an army of legal / regulatory experts focused on this event. Its not bad you considered this but it distracted me after such a strong start for why your cyber recommendations are so important. • Could have had more ties to risk in high priority recommendations. • Team members names should be listed on the title slide. Did not state the contributions of the other team members. It would be best to provide specifics they contributed or provide job roles or titles. • It is recommended to provide job roles or titles or clarity which team members participated in which aspects of the work. • The loss of revenue should be quantified. • When reading slides or scripts it is best to read at a pace to allow the view to process the content and read the slides. Mitigation

Strong Points	*Areas of Improvement*
	slides were read at too fast of a pace for comprehension. • Mitigation should also discuss price, staffing, software/hardware • Auditing and training is not necessarily free. It could be conducted by consultants and conducted by current staff it still has cost associated with the staff work time. • SIEMs will require staff and implementation plan, etc.

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	0	125	0	0	125

Whack a Mole		
WAM1	WAM2	WAM3
250	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
1450	27

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	23	27	27	25	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
2407.72	5.35%

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
1227

Green Team Survey Comments
• footer not included in home page • footer not included in home page • Keep up the good work! • The logos are not in the required positions. • Website failed to load. • site does not load • 504 gateway time out • Met all the requirements. Good job! • Looks good, keep it up! • Good job • Rock-solid work! Even Obsidian Rifts rigs approve" Unfortunately, you're missing the footer on the login and signup pages. • Good work! All intended areas are still accounted for within the website and no issues locating anything per the requirements. Your rid status does say 'Not Operational'. • looks good • Site is down