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

DAKOTA STATE UNIVERSITY

DAKOTA STATE UNIVERSITY

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 76 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	812	54.13%	5
Security Documentation	1093	87.44%	41
C-Suite Panel	1095	87.60%	19
Red Team	1125	45.00%	35
Blue Team	1696	84.80%	52
Green Team Surveys	1500	100.00%	23
Deductions	0		
Overall	**7321**	**73.21%**	**23**

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	812

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

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

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	Yes
11.7	Yes
12	No
13	
14	
15	Yes
16	Yes

17	Yes
18	Yes
19	Yes
20	Yes
21	
22	
23	
24	Yes
25	
26	
27.1	No
27.2	Yes
28	Yes
29	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	1093

Strong Points	*Areas of Improvement*
• Vulnerability coverage is complete and every fix is justified with technical detail. • Very comprehensive list of known vulnerabilities. • Your system hardening section was detailed and well thought out. The explanations showed strong understanding and reflected good decision-making throughout the process. • System Hardening is detailed and organized well into chronological sections with justification for actions.	• Split longer sections and tables for easier reading. Add more headings and visual separation for clarity. • System overview only discussed machines involved in the system and didn't address the overall system and its purpose. • A small improvement would be adding clearer descriptions of the mitigations when listing vulnerabilities. You demonstrated strong grasp of the material, and with slightly more explanation in that section your documentation would feel even more complete.

Strong Points	*Areas of Improvement*
• Asset Inventory, Network Diagram, and Hardening Recommendations	• Keep your hostnames consistent. Try to reword the System Overview to target senior leadership and explain terminology when used (what's a domain?). When you list CVEs, it's helpful to also write out what the vulnerability is. • No notes of improvement at this time

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	1095

Strong Points	*Areas of Improvement*
• Intro music - very nice touch. Excellent introduction. Excellent rollout of strategy to reduce risk. Purdue Model - no other team mentioned this. Far fewer negatives that all other teams - very well done! • Risks Related to Operational and Business Concerns (30%): The team provided a clear summary of business and operational risks. They successfully identified how the incident (a contractor's remote access credential compromise) affected the company's concerns and bottom line (finances). Specific financial impacts were quantified, including losing roughly 3 to $5 million for equipment failure (compressor replacement). The discussion of reputational damage reduced stakeholder confidence, and significant risk to personnel safety was appropriate for the C-Suite. • Strategy to Reduce Risks (30%): The strategy was complete and comprehensive. It included three or more long-term action items, such as isolating compromised units, restoring clean configurations, implementing the Purdue model, securing remote access via multifactor authentication (MFA), segmenting the ICS from enterprise IT, and delivering focused staff training. This detailed plan clearly addressed the identified risks, protecting operational uptime, equipment reliability, and personnel safety. • High Priority Recommendations (30%): The team provided four high priority	• Did not introduce the team at the beginning nor did the team introduce themselves when they gave their part of the presentation. No timeline shown not summary of costs - C-Suite uses both to get a snapshot of the fix. • Quality of Presentation (Visual Aids): The presentation's visual aids were a bit wordy and lacking graphs and charts. While the team was well dressed, visual aids must have a consistent, professional appearance to reach the Exemplary level. In a C-Suite briefing, slides should minimize text and maximize visual impact through elements like graphs, charts, and clear diagrams to help non-technical executives quickly grasp complex information. Reducing the wordiness of the slides would make the visual aids more acceptable for a C-Suite audience. • If not stated verbally could be included in text over slides • For strategies and recommendations also include cost, staffing and training requirements, and hardware and software requirements. • Jargon and acronyms should be explained • Could include references on last slide and list of related software and hardware recommendations" • Recommendations could be more quantified (financial analysis of prevention costs versus risks) and tailored to Obsidian Rift Energy's specific environment. Vendor

Strong Points	*Areas of Improvement*
recommendations (MFA/VPN Segmentation, Network Monitoring, Staff Awareness/Drills, and Backup/Disaster Recovery Policy). Complete and consistent reasoning was provided for all four actions. Crucially, the team adhered to the requirement that actions must require at most a minimal level of additional funding by mentioning the deployment of Snort intrusion detection software (an open-source tool). The team's focus on low-cost, high-impact solutions demonstrates a strong understanding of the limited funding constraint. • Team Acknowledgment: The team exceeded the minimum participation requirements. All six members were acknowledged for their specific contributions, including script writing, core business strategy, high priority actions, reviewing, and video editing, demonstrating a clear acknowledgment of contributions from all team members. The team also met the criterion for appropriate dress code, as they were described as well dressed • Nice use of background music • Good use of video embedded over slides • Good work stating the names of the team members and their roles • Good work quantifying loss • Covered details required for all categories but missing financial details. • Good job at quantifying the impact of risks. • Very professional presentation.	management and risks could be more specific. • Your listed risks are largely just impacts, which is only one part of the equation for risk. Your strategy is really just high priority recommendations. Strategy should be long term goals that drive actions that reduce the overall risks you talk about. What are the costs for your high priority recommendations? How do the recommendations drive your strategy? How do they reduce the risks you convey? • Try not to use too much jargon when explaining your operational risk mitigations to the C-Suite

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	125	125	0	0	250

Whack a Mole		
WAM1	WAM2	WAM3
250	125	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
1480	216

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	26	27	27	27	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
18925.89	42.06%

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
1500

Green Team Survey Comments
• Good Job!!! • Very Good!