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

PURDUE UNIVERSITY MAIN CAMPUS

BTAP

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 11 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	716	47.73%	11
Security Documentation	1117	89.36%	31
C-Suite Panel	1085	86.80%	25
Red Team	1250	50.00%	27
Blue Team	1752	87.60%	46
Green Team Surveys	1412	94.13%	22
Deductions	0		
Overall	**7332**	**73.32%**	**22**

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	716

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

1	Yes	10.7	Yes	17	Yes
2	Yes	10.8	Yes	18	Yes
3	No	10.9	Yes	19	Yes
4	Yes	11.1	Yes	20	Yes
5	Yes	11.2	Yes	21	
6	No	11.3	Yes	22	Yes
7	No	11.4	Yes	23	
8		11.5	Yes	24	
9	No	11.6	Yes	25	Yes
10.1	Yes	11.7	Yes	26	No
10.2	Yes	12	No	27.1	Yes
10.3	Yes	13	No	27.2	Yes
10.4	Yes	14		28	Yes
10.5	Yes	15	Yes	29	Yes
10.6	Yes	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	1117

Strong Points	*Areas of Improvement*
• A strong list of vulnerabilities was provided. • The team did a great job identifying vulnerabilities and mitigations, and had very good system hardening recommendations. • Great mix of technical and managerial clarity. • Covered great amount of details with clarity and looking good to present. Overall great effort by the team specially in the vulnerability listing section.	• The asset inventory and network diagram were not as strong as the rest of the document. • The team's asset inventory should list specific OS versions. Some services were also not present. • The asset table could have used a few more service details. • Missing and mismatch information - i.e. once the issue is highlighted in system overview, would need more clarity.

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	1085

Strong Points	*Areas of Improvement*
• Nice high level summary of timeline and costs • The team demonstrated a clear understanding of the Abyssal Pearl incident, effectively identifying the associated risks, their potential business impact, and practical measures to mitigate those risks. • Great high-priority actions; network segmentation is the #1 in my book too! • well-done slides and presentation though a bit rushed • Excellent detailed information regarding flow, safety logic and risk. Mentioning of regulatory bodies and strategies was great. Slides are clear, concise and easy to follow. • Team did a great job equating the scenario to real life cyberattacks. Also did a very nice job explaining financial and reputational risks in the very beginning. Presentation was clear and well thought out.	• More understanding of costs associated to operations and business risks • Presentation met all rubric criteria at a high level. The only minor area for improvement would be increasing confidence and projection during delivery to ensure clarity and presence match the strength of the team's content. • It would have been great to hear about how the non-presenting team members contributed, and a better breakdown of the hours required to implement specific security controls • Monetary value is important to the C-suite, give room for C-suite to ask questions if they have • Information was great. Speaking a little fast during presentation. • A brief summary at the end of the presentation would have tied all of the talking points together.

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	250	0	250	0	125

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
1475	277

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
24205.12	53.79%

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
1412

Green Team Survey Comments
• Footer is not at the bottom of the page, heading is incorrect
• company name not right,
• Excellent work!
• Good Job!!!
• Site is down