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

# THE UNIVERSITY OF TEXAS AT DALLAS

## CYBER BLUE TEAM

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 19 SCORECARD

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

| Score Category | Team Points | Percent of Points | Team Ranking |
|---|---|---|---|
| Anomalies | 500 | 33.33% | 34 |
| Security Documentation | 1067 | 85.36% | 47 |
| C-Suite Panel | 1102 | 88.16% | 17 |
| Red Team | 1250 | 50.00% | 27 |
| Blue Team | 1777 | 88.85% | 42 |
| Green Team Surveys | 924 | 61.60% | 39 |
| *Deductions* | 0 | | |
| **Overall** | **6620** | **66.20%** | **39** |

## 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 | 500 |
|---|---|

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 | | 10.9 | | 19 | Yes |
| 4 | Yes | 11.1 | Yes | 20 | Yes |
| 5 | Yes | 11.2 | Yes | 21 | |
| 6 | | 11.3 | Yes | 22 | |
| 7 | | 11.4 | | 23 | |
| 8 | | 11.5 | | 24 | |
| 9 | No | 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 | 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 | 1067 |
|---|---|

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • Good explanations appropriate for C-suite<br>• system overview provides an excellent summary catered to senior audience<br>• The network diagram was excellent. | • System hardening steps were adequate but could be given a stronger justification and include long term. Tools used were explained but there was no list provided.<br>• incomplete mitigation for HMI and PLC<br>• Would have been good to remove the template. |

### 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 | 1102 |
|---|---|

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • I was especially impressed with both the Risk Mitigation Strategy and High Priority Recommendations slides that this team created bar charts on the Cost Estimates both for the Initial Setup Costs and the Yearly Upkeep Costs. As a member of senior leadership, this graphic that quickly allows me to digest a lot of information is invaluable to the decision-making process. Kudos to this team for taking the time to research and parse out what would be the front-end and recurring costs for each of these recommendations!<br>• Good thorough capture of operational and business risks<br>• Clear quantification of financial loss and legal implications. Presentation connects safety and revenue risk well.<br>• Great explanation and able to link beneficial between C-Suite and financial improvement of the company<br>• Both presenters were professionally dressed. The slides were easy to read.<br>• The team provided a well-defined mitigation strategy with clear, actionable steps. Their time was used effectively, and they showed a solid understanding of how to reduce the identified risks. | • While the Incident Overview felt nuanced and descriptive, the Business and Operational Risks by comparison felt vague and amorphous. Other than the specific of ""$124,000/day loss in oil revenue alone,"" the rest of these feel non-specific and general. It would be great to offer graphic specifics that parse out the specific risks at stake here rather than categories that many unrelated risks could fall under.<br>• Furthermore, when the slides and speaker shift, the opposite happens, where the language and details for Risk Mitigation Strategy and High Priority Recommendations are so specific that much of these insights would be lossed on all but the most technical members of the audience. While costs and risk are applicable to all in leadership, jargon like SIEMs, access controls, hardening, virtualization, role-based access, etc. would likely put off many of those you are trying to connect with. Ensure that your language is accessible to all of those in business, not just the CIO and CTO.<br>• What were the additional team members' contributions? Individual slides were too packed, reduce the amount of text or spread among more slides. More direct, not implied, correlation on how the strategy and high priorities reduce operational and business risks.<br>• Strategy section lists actions but lacks sequencing or justification of effectiveness beyond general prevention.<br>• The presentation was short, which could have easily been remedied by the speakers watching out quickly they were speaking. The font size in the presentation make the slide a little hard to read.<br>• Overall, the presentation met rubric expectations. To strengthen future presentations, the team could improve the visual aids to make the content more engaging and visually cohesive, helping key points stand out more clearly. |

## 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 | 0 | 250 | 125 | 0 | 0 | 250 |

| Whack a Mole | | |
|---|---|---|
| WAM1 | WAM2 | WAM3 |
| 250 | 0 | 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 |
|---|---|
| 1455 | 322 |

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 | 24 | 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 |
|---|---|
| 28167.50 | 62.59% |

## 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 |
| --- |
| 924 |

| *Green Team Survey Comments* |
| --- |
| • no admins<br>• no admins<br>• Positions of interest cannot be applied for, admin users are not there, logos are not in the header.<br>• no admins, logos, careers<br>• no logos, jobs changed, blue admin gone<br>• incomplete career page, none assigned admin. no logo.<br>• Did not see admin tags after admin sign in. Did not see blue team either.<br>• "No Open positions No Header Logo"<br>• Logos not in header, no careers listed on careers page<br>• Hello Team 19. There were a couple things that needed to be completed to get a perfect score. The header was missing the ObsidianRift and a logo for the Abyssal Pearl within the site navigation bar. The users 'blue@obsidianrift.oil' and 'green-admin@obsidianrift.oil' should have the admin tags. Lastly, there should have been a section of positions of interest that can be applied for.<br>• The admin users were not tagged with admin, also the logs were not in the header. Good luck!<br>• Site does not load<br>• website does not load<br>• Unable to load<br>• No logos in the header, missing footer on all pages, missing admin users in the admin panel, and no open positions listed.<br>• no open positions, Blue Admin not showing in user management, no logos in header<br>• Site is down |