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

# COLORADO SCHOOL OF MINES

## ORESEC

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 65 SCORECARD

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

| Score Category | Team Points | Percent of Points | Team Ranking |
|---|---|---|---|
| Anomalies | 634 | 42.27% | 18 |
| Security Documentation | 901 | 72.08% | 72 |
| C-Suite Panel | 1109 | 88.72% | 14 |
| Red Team | 750 | 30.00% | 53 |
| Blue Team | 1823 | 91.15% | 34 |
| Green Team Surveys | 1392 | 92.80% | 42 |
| *Deductions* | 0 | | |
| **Overall** | **6609** | **66.09%** | **42** |

## 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 | 634 |
|---|---|

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

| | | | | | |
|---|---|---|---|---|---|
| 1 | No | 10.7 | Yes | 17 | Yes |
| 2 | | 10.8 | Yes | 18 | Yes |
| 3 | No | 10.9 | | 19 | Yes |
| 4 | Yes | 11.1 | Yes | 20 | Yes |
| 5 | Yes | 11.2 | Yes | 21 | Yes |
| 6 | No | 11.3 | Yes | 22 | Yes |
| 7 | | 11.4 | Yes | 23 | |
| 8 | No | 11.5 | Yes | 24 | |
| 9 | Yes | 11.6 | | 25 | |
| 10.1 | Yes | 11.7 | | 26 | |
| 10.2 | Yes | 12 | | 27.1 | No |
| 10.3 | Yes | 13 | | 27.2 | No |
| 10.4 | Yes | 14 | | 28 | No |
| 10.5 | Yes | 15 | Yes | 29 | Yes |
| 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 | 901 |
|---|---|

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • Good inventory and network diagram.<br>• The hardening process shows solid organization and a thoughtful approach that uses multiple layers of defense and strong monitoring tools.<br>• Good job on being consistent between the asset inventory and network diagram.<br>• Covered great amount of details with clarity and looking good to present. Overall great effort by the team. | • More vulnerabilities needed to be listed, and the hardening needed to be a broad action plan.<br>• Some mitigations were left pending; finishing and verifying those fixes would make the documentation and results stronger.<br>• System hardening is the overall actions to better secure your system and more than just what you did to each machine for discovering and removing vulnerabilities.<br>• Vulnerability list is missing details. |

## 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 | 1109 |
|---|---|

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • great introduction<br>• As a whole, the team presented incredibly well with each member having an opportunity to present information. They spoke clearly, had no visual distractions, and kept the video to just slightly over 5 minutes.<br>• The high priority recommendations would improve the overall security and protect business continuity. The recommendations were presented in a complete and consistent manner with reasoning provided for each recommendation.<br>• Exceptional Risk Analysis (30% Weight): Team 65 provided a clear summary of business and operational risks, including physical risk (catastrophic safety incidents), business risk (significant financial loss and reputation damage), and cyber security risk (log manipulation, lateral movement). The analysis clearly identified how these risks affect ObsidianRift Energy Co.'s concerns and their bottom line (finances). The presentation was appropriate for the entire C-Suite audience, avoiding excessive technical jargon.<br>• Complete Strategy (30% Weight): The team provided a complete, logical strategy consisting of three key long-term action items: introducing a disaster recovery plan (to increase response/recovery time), ensuring an improved security posture (proper vetting of third-party contractors), and implementing proper employee training. This strategy clearly addresses the previously identified risks.<br>• Quality of Presentation (8% Weight): The team utilized clean good slides, which demonstrated a consistent and professional appearance.<br>• Clearly outlined business risks and operational impact following an industrial control system compromise, with direct ties to reputation, safety, and production. | • more information on the slides<br>• Some of the recommendations require significant additional investment. A saving grace is that some open-source tools are recommended to save costs elsewhere.<br>• Adherence to Funding Constraints (High Priority Recommendations - 30% Weight): To achieve the Exemplary (Level 4) score, the high-priority recommendations must require at most a minimal level of additional funding, ideally using only free or open-source tools. While the team successfully leveraged cost-saving open-source tools like Goofish (for phishing training) and WAZA (for SEIM log collection/intrusion detection), they explicitly noted that the installation of backup analog equipment represents a ""necessary expense"" requiring additional investments. Future presentations should strive to justify all 3-4 recommendations using strictly minimal or zero-cost solutions to maximize the score in this category.<br>• Presentation Requirements (2% Weight): Although six members presented, the judges look for two or more active team members to participate equally. The team noted that members did not have the same amount of presentation time, and some had to talk fast cause of time. Ensuring a more even distribution of speaking roles and strictly maintaining the presentation length to approximately five (5) minutes will meet the Exemplary standard. The video length of 5 minutes and 23 seconds was also slightly too long.<br>• Vendor management could be more specific.<br>• A bit on the technical side, where lateral movement may not be needed.<br>• While the strategy is sound and looks longer term, you don't make a strong connection to how your strategy will reduce the specific risks you call out. For high priority recommendations, tie them back to the |

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • Very strong. The price timeline for the remediation strategy was great!<br>• Good job articulating the risks, instead of just talking about he incident. | strategy and original business risks. How do they reduce risk right now? |

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

| 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 | 348 |

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 |
|---|---|
| 30475.81 | 67.72% |

## 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 |
|---|
| 1392 |

| *Green Team Survey Comments* |
|---|
| • Footer is visible on all pages except the homepage |
| • Header formatting is not consistent between the home page and other pages. The company name shifts positions. |
| • No admin button when logged in |
| • footer not available on main page |
| • footer not visible on main page |
| • you don't have a footer on the front page. Otherwise, you're doing great! |
| • Rock-solid work! Even Obsidian Rift's rigs approved just slap that missing homepage footer on and you're golden! |
| • Address footer is supposed to be on every web page, but it's not found on the home. |
| • Good job - may want to put the footer on the home page - but it is on the others. |
| • Hello Team 65 the footer text was missing on your main page. |
| • footer missing from main page |
| • 5:53 This site can't be reached |