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

# GEORGIA INSTITUTE OF TECHNOLOGY

## CYBER JACKETS 2

### 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 7 SCORECARD

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

| Score Category | Team Points | Percent of Points | Team Ranking |
|---|---|---|---|
| Anomalies | 304 | 20.27% | 75 |
| Security Documentation | 1226 | 98.08% | 3 |
| C-Suite Panel | 1102 | 88.16% | 17 |
| Red Team | 500 | 20.00% | 70 |
| Blue Team | 1485 | 74.25% | 66 |
| Green Team Surveys | 930 | 62.00% | 66 |
| *Deductions* | 0 | | |
| **Overall** | **5547** | **55.47%** | **66** |

## 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** | 304 |

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

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

| | |
|---|---|
| 10.7 | |
| 10.8 | |
| 10.9 | |
| 11.1 | |
| 11.2 | |
| 11.3 | |
| 11.4 | |
| 11.5 | |
| 11.6 | |
| 11.7 | |
| 12 | No |
| 13 | No |
| 14 | |
| 15 | |
| 16 | Yes |

| | |
|---|---|
| 17 | Yes |
| 18 | Yes |
| 19 | Yes |
| 20 | Yes |
| 21 | No |
| 22 | |
| 23 | |
| 24 | Yes |
| 25 | |
| 26 | |
| 27.1 | No |
| 27.2 | No |
| 28 | No |
| 29 | No |
| 30 | |

## 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** | 1226 |

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • Good inclusion of the ICS data flows. Great justifications for system hardening, with a good focus on the potential impacts if patched vs unpatched.<br>• formatting makes it easy to go through the document; great job with making connections in network diagram<br>• Super professional.  References frameworks and justifies everything.<br>• Comprehensive Vulnerability Identification: The team demonstrated outstanding technical effort by identifying an exceptionally high volume of vulnerabilities | • A lot of extra ports that could have been disabled, while some important ports are missing from the asset inventory. Known Vulnerabilities section is missing clear language that the PLC and CNC/HMI are future patch recommendations.<br>• more explanation separated for each initiative of system hardening<br>• Could use a brief summary table or visual to make it easier to digest.<br>• Completeness of Required Services: Although the team listed all six hosts and dozens of services, the Asset Inventory |

| *Strong Points* | *Areas of Improvement* |
|---|---|
| across all six systems (significantly exceeding the vulnerabilities required for an Exemplary score). Crucially, the documentation provided an appropriate mitigation for every single vulnerability listed, including strategies for issues that currently had ""no known solution"" (unpatched vulnerabilities). This detailed, processed presentation successfully targeted the required ""senior leadership"" audience.<br>• Strategic System Hardening: The hardening section was highly comprehensive and expertly justified. The team exceeded expectations by outlining their strategy using six distinct focus areas (e.g., Patch Management, Access Controls, Risk Reduction). Furthermore, the justification for these steps was strong, referencing established, well-accepted best practices such as NIST SP 800-82 Rev. 3 and CISA's ICS Recommended Practices.<br>• Detailed Network Diagram: The Network Diagram included was exemplary, displaying all six assets, providing logical network structure (10.0.5.128/26 subnet), and clearly illustrating logical connections and data flow paths (e.g., Modbus Data Flow between HMI and PLC, and Historian Data Flow between the Webserver and Database). | appears to have missed two of the mandatory required services/ports established in the competition requirements, specifically SNMP (161) on the Public Database and SMTP (25) on the Task Box. Listing ""All"" services (90%+) is necessary to achieve the maximum ""Exemplary"" score. Missing mandatory services drops the score to the Proficient range (70%+) in this category, even with otherwise exhaustive detail.<br>• Consistency Check: Moving forward, the team should implement a final cross-check of their Asset Inventory table against the explicit competition list of Required Services and Port Numbers (found on page 8 of the competition expectations document). This ensures that every mandatory scoring element is present, regardless of how many additional services were identified, securing the full score for this required component. |

## 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* |
|---|---|
| • Justification of recommended actions via the cost of inaction was a nice twist.<br>• Fantastic job with the overall presentation, you had strong details on effective strategies to reduce business risks. Great work!<br>• The presentation slides were very easy to understand, and clear direction was provided. There was a great perspective on the cost of not performing action related to | • Identified risks should be differentiated from impact and not expressed as merely as consequences of the incident. n r. The strategy lacked clear connections to the previously identified risks in most cases. Differentiate between strategies and high priority recommendations.<br>• An area for improvement would be to include more details on operational risks |

| *Strong Points* | *Areas of Improvement* |
|---|---|
| this situation. It is an important step when meeting with leadership to let them know what the ask is of them. You need to be clear with that.<br>• Layout was easy to follow. I like that you draw attention to loss of profit. When dealing with a widget that fluctuates in price such as oil, consider using a higher average cost in your calculations. Current oil prices are on the lower end, you can strengthen your position using average cost on the year or even just peak travel season when demand is high.<br>• This is a well thought out, professionally developed and delivered presentation. Each team member spoke clearly and had roughly equal allotments of time to present information.<br>• the presentation was clear and concise, it used minimal/no industry jargon, which makes it easy for a non technical person to understand problem statement and solutions. | and their impact on the company's concerns and financial performance.<br>• The presentation was good but very scripted and did not have a lot of energy to draw in the viewer. Allow yourself to go off script and to share your points as part of a conversational tone. Also, dive a little more into the financials and how you came to your decisions as the cost impact of an event is always a deep conversation with leadership.<br>• Be sure to proof the final video, you have a + sign on each slide that was noticeable.<br>• I struggled with grading the strategy to reduce business risks because the team put together a good risk mitigation framework, explained it clearly, and gave 4 action items however the strategy is explained within a 30-day window and that isn't considered "long term".<br>• two points, they provide a 30 day strategy to resolve issue but no clear long term solution. for example, Training was mentioned but only would be provided at onboarding, its not clear if annual trainings to employees would be provided. |

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

| Whack a Mole | | |
|---|---|---|
| WAM1 | WAM2 | WAM3 |
| 125 | 125 | 0 |

## 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 |
|---|---|
| 1220 | 265 |

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) |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 27 | 27 | 26 | 27 | 18 | 27 | 27 | 19 | 19 | 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 |
|---|---|
| 23177.77 | 51.51% |

## 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 |
|---|
| 930 |

| *Green Team Survey Comments* |
|---|
| • Name spelled incorrectly and logos too small. careers missing descriptions. footer missing on main page<br>• ObsidianRift Energy Co. should be the name in the header. can not select a position to apply for. Footer not on home page.<br>• When applying I can't pick what position to apply for and warning you have a red member with admin access!!!!<br>• footer not showing on home page. Address not correct<br>• Header is incorrect, cannot apply for specific positions, footer is not on home page.<br>• "No footer on the main, singup, and login pages. None of the career options are listed. User name Red had Admin which should not have."<br>• Homepage needs a footer. Title says Obsidian Energi Co |

| *Green Team Survey Comments* |
|---|
| • Address footer is supposed to be on every web page, but it's not found on the home.<br>• Could not scroll down the homepage to verify the text at the bottom of the page.  Good luck!<br>• Company name in nav bar reads 'Obsidian Energi Co.'. Careers page has the positions listed under 'Open Positions', but not under 'Positions of Interest'. Requirements were met for user management, but there is an additional admin. No footer on home page, Login, or Sign Up.<br>• Webpage did not load. Error message: 504 Gateway Time-out<br>• website will not load<br>• "504 Gateway Time-out nginx/1.19.0"<br>• website not loading<br>• Footer not on every page and no way to pick point of interest when apply<br>• Site is down |