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

# ILLINOIS INSTITUTE OF TECHNOLOGY

## IIT CYBERHAWKS

November 9, 2024

In-Person

| Number of Teams | Max Team Points Received | Min Team Points Received | Mean Team Points Received | Total Points Possible |
|---|---|---|---|---|
| 94 | 9153 | 1350 | 6115.31 | 10,000 |

## TEAM 49 SCORECARD

This table highlights the *team's* efforts for the 2024 CyberForce Competition®.

| Score Category | Team Points | Percent of Points | Team Ranking |
|---|---|---|---|
| Anomalies | 659 | 32.95% | 44 |
| Security Documentation | 896 | 89.60% | 27 |
| C-Suite Panel | 831 | 83.10% | 50 |
| Red Team | 1019 | 40.76% | 62 |
| Blue Team | 1780 | 89.00% | 63 |
| Green Team Surveys | 434 | 28.93% | 60 |
| *Deductions* | 0 | | |
| Overall | **5619** | **56.19%** | **60** |

## 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. Most anomalies are mapped to the NIST NICE Framework and fall into one of seven work role categories: *Oversight & Governance, Design & Development, Implementation & Operation, Protection & Defense, Investigation, Cyberspace Intelligence, and Cyberspace Effects. Some anomalies may also be categorized as Energy or "Other".* For those mapped to the NIST NICE Framework, their will include the mapping to associated knowledge, skill, ability, and task roles within its respective category, offering students with a comprehensive idea of the wide range of responsibilities cybersecurity professionals face while in the field.

| Anomaly Score | 659 |
|---|---|

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

| | | | | | |
|---|---|---|---|---|---|
| 1 | yes | 27 | Not Answered | 53 | Not Answered |
| 2 | yes | 28 | Not Answered | 54 | yes |
| 3 | yes | 29 | Not Answered | 55 | yes |
| 4 | yes | 30 | Not Answered | 56 | no |
| 5 | yes | 31 | no | 57 | yes |
| 6 | yes | 32 | Not Answered | 58 | yes |
| 7 | yes | 33 | Not Answered | 59 | yes |
| 8 | yes | 34 | yes | 60 | Not Answered |
| 9 | no | 35 | no | 61 | Not Answered |
| 10 | yes | 36 | Not Answered | 62 | yes |
| 11 | Not Answered | 37 | yes | 63 | yes |
| 12 | Not Answered | 38 | yes | 64 | no |
| 13 | no | 39 | yes | 65 | no |
| 14 | yes | 40 | yes | 66 | Not Answered |
| 15 | no | 41 | Not Answered | 67 | Not Answered |
| 16 | yes | 42 | Not Answered | 68 | yes |
| 17 | yes | 43 | Not Answered | 69 | Not Answered |
| 18 | yes | 44 | Not Answered | 70 | yes |
| 19 | yes | 45 | yes | 71 | Not Answered |
| 20 | Not Answered | 46 | yes | 72 | Not Answered |
| 21 | no | 47 | no | 73 | Not Answered |
| 22 | yes | 48 | yes | 74 | Not Answered |
| 23 | Not Answered | 49 | Not Answered | 75 | Not Answered |
| 24 | Not Answered | 50 | Not Answered | 76 | yes |
| 25 | Not Answered | 51 | Not Answered | 77 | yes |
| 26 | Not Answered | 52 | Not Answered | | |

## 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 | 896 |
|---|---|

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • Your system hardening goals are clearly stated and well reasoned.<br>• Well designed document and network diagram<br>• Your report was very thorough and concise. Your asset inventory and vulnerabilities and mitigations were very thorough, and your hardening report was clearly laid out and easily understood.<br>• As this report is going to be reviewed by leadership, the acronyms should be spelled out before first use. The acronyms CNC and PLC. The device and software descriptions are proper nouns, so it's ok to not spell them out. For future, utilities have started using the word "component" instead of device to identify it as part of the Industrial Control System.<br>• The Asset Inventory is well done. It may help to have a small discussion about why the hosts have duplicate IP addresses. This could be confusing to a non-technical person. I had to think hard about why some components had multiple IP addresses when I saw that. In my experience I had to really think about why some components had multiple IP addresses.<br>• The System Harding Strategy has an excellent balance between technical and non-technical information.<br>• | • Find a different way to display or report your asset inventory that doesn't repeat the same information so many times in the table format.<br>• Did not identify most vulnerabilties.<br>• You network map could have more resembled the asset inventory and you could have shown the connections between the machines. Also there was no reason for bullets in your system overview, would have read better with just paragraphs.<br>• The network diagram is extremely clear and uses graphics that are instantly understood. Its not clear whether vulnerability mitigations have been mitigated (workaround) and when the remediation (permanent solution) will be done.<br>• The use of the word "make" will probably be seen as controversial. As softer word might be "require" or that a policy will be written (to do the thing).<br>• Finally, although the vulnerabilities are technically and correctly written, an upper levels of manage won't be able to read this easily. It may help to "generalize" the vulnerability description. For example: on the host "mysql database gives permissions: GRANTSELECT, INSERT, UPDATE, DELETE,CREATE, DROP, REFERENCES, INDEX,ALTER, CREATE TEMPORARY TABLES, LOCKTABLES, CREATE VIEW, SHOW VIEW,CREATE ROUTINE, EVENT, TRIGGER,DELETE HISTORY ON `test\_%`.* TOPUBLIC) might be generalized to: "The DB have additional security features that will improve the protection of the Host/System." I'm sure the team will have better ideas on how to generalize the vulnerability so that upper level management has the concept and |

| | |
|---|---|
| | then quickly understand how the Mitigation/remediations will contribute to the to the overall security program. In addition, I've seen that most upper level management will very much appreciate that the vulnerability is more generalized. I've had more than one manager that has made that comment after I've done an assessment for them. |

### 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** | 831 |

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • Good use of embedded speaker video over slides. Good discussion of ICS systems,in addition to IT systems.<br>• Clarity of presentation<br>• Effectively incorporated business terminology in the recommendation section.<br>• You explained the risks of not following the priorities listed. Overall a professional presentation. | • Third speaker volume is very low. It is recommended to adjust audio to match across speakers. Automated tools - more details needed, price and is staffing required. For high priority activities, will need staff be hired? There is a mention of a SOC, but not of staffing the SOC.<br>• More ties to the financial risk<br>• I suggest minimizing the use of technical jargon when discussing business risks and placing greater emphasis on customer impact.<br>• While you did explain concerns to the business, they came across as mostly technical/security risks. The C-Suite will mainly want to hear about financial risks.<br>• The C-Suite would better be informed with an explanation of how the strategy directly addresses business concerns. |

## RED TEAM SCORING

### RED TEAM FLAG INPUTS (ASSUME BREACH & WHACK A MOLE)

This year we will be using ***Assume Breach*** for part of your Red team score. This will be worth *1000 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 | AB8 | AB9 | AB10 |
| 50 | 100 | 75 | 25 | 100 | 0 | 75 | 50 | 0 | 0 |

| Whack a Mole | |
|---|---|
| WAM1 | WAM2 |
| 93 | 0 |

### AUTOMATED SCRIPT CHECK – VULNERABILITY

This portion of the Red team score will be worth *750 points*. This will be done via an automated scripted check.

| Automated Script Score | 450 |
|---|---|

## 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 | AI Algorithm Score |
|---|---|
| 1380 | 400 |

## 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 |
|---|
| 434 |