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

# IDAHO STATE UNIVERSITY

## WIRESPUD

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 94 SCORECARD

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

| Score Category | Team Points | Percent of Points | Team Ranking |
|---|---|---|---|
| Anomalies | 798 | 39.90% | 29 |
| Security Documentation | 628 | 62.80% | 75 |
| C-Suite Panel | 950 | 95.00% | 5 |
| Red Team | 719 | 28.76% | 79 |
| Blue Team | 1490 | 74.50% | 79 |
| Green Team Surveys | 903 | 60.20% | 63 |
| *Deductions* | 0 | | |
| Overall | **5488** | **54.88%** | **63** |

## 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 | 798 |
|---|---|

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

| | | | | | |
|---|---|---|---|---|---|
| 1 | yes | 27 | no | 53 | yes |
| 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 | Not Answered | 60 | yes |
| 9 | yes | 35 | Not Answered | 61 | yes |
| 10 | yes | 36 | Not Answered | 62 | yes |
| 11 | no | 37 | no | 63 | yes |
| 12 | yes | 38 | Not Answered | 64 | no |
| 13 | no | 39 | no | 65 | Not Answered |
| 14 | yes | 40 | yes | 66 | Not Answered |
| 15 | no | 41 | Not Answered | 67 | Not Answered |
| 16 | yes | 42 | Not Answered | 68 | Not Answered |
| 17 | yes | 43 | no | 69 | Not Answered |
| 18 | yes | 44 | Not Answered | 70 | yes |
| 19 | yes | 45 | yes | 71 | yes |
| 20 | yes | 46 | yes | 72 | yes |
| 21 | yes | 47 | yes | 73 | yes |
| 22 | yes | 48 | yes | 74 | yes |
| 23 | yes | 49 | Not Answered | 75 | Not Answered |
| 24 | no | 50 | yes | 76 | yes |
| 25 | Not Answered | 51 | yes | 77 | yes |
| 26 | Not Answered | 52 | 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 | 628 |
|---|---|

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • I liked how the network diagram clearly identified the assumed breach.<br>• Reasonable mitigations for the identified vulnerabilities.<br>• Got most of the key points of the network.<br>• Network diagram was the best I've seen! Very detailed and well made. | • Formatting throughout. Some content was missing, the content you do have should be consistent.<br>• There is a lack of thorough examination at some places in the document. Try to imagine sending this to senior leadership and the information they would want from a professional document. Also, make sure fonts are the same throughout the document and diagrams are highly interpretable/not cluttered.<br>• Expand on the base knowledge to provide reasoning and show knowledge of the network.<br>• System hardening steps were not clearly defined. It read more like what you did to fix vulnerabilities as opposed to steps/procedures generally taken to harden your systems.<br>• Always avoid empty boxes, especially in asset inventory. |

### 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 | 950 |
|---|---|

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • Overall great presentation and relating back to standards is well done.<br>• Very logical and professional presentation! Well done.<br>• The presentation quality was excellent very professional and informative, providing a detailed overview of the three key points.<br>• This presentation was outstanding. Very profesionnal and thoughtful with great attention to detail. | • Mentioning 800-53 for OT network segregation is great but 800-53 is IT focused. Could dive deeper and mention using 800-82r3 for securing the OT network.<br>• My only perfect score so no recommendation here.<br>• no comment<br>• Make sure your strategies are clear and concise, as they're meant to be long term directions. Also, be careful when talking |

| | |
|---|---|
| | about specific NIST codes that the C-Suite isn't familiar with. |

## 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 |
| 0 | 50 | 50 | 0 | 0 | 25 | 0 | 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 |
|---|---|
| 1390 | 100 |

## 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 |
|---|
| 903 |