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

# NORTHEASTERN UNIVERSITY

## NUCCDC

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 60 SCORECARD

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

| Score Category | Team Points | Percent of Points | Team Ranking |
|---|---|---|---|
| Anomalies | 1410 | 70.50% | 4 |
| Security Documentation | 525 | 52.50% | 80 |
| C-Suite Panel | 505 | 50.50% | 90 |
| Red Team | 1256 | 50.24% | 45 |
| Blue Team | 1965 | 98.25% | 47 |
| Green Team Surveys | 1413 | 94.20% | 29 |
| *Deductions* | 0 | | |
| Overall | **7074** | **70.74%** | **29** |

## 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 | 1410 |
|---|---|

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

| | | | | | |
|---|---|---|---|---|---|
| 1 | yes | 27 | Not Answered | 53 | yes |
| 2 | yes | 28 | yes | 54 | yes |
| 3 | yes | 29 | no | 55 | yes |
| 4 | yes | 30 | yes | 56 | no |
| 5 | yes | 31 | yes | 57 | yes |
| 6 | yes | 32 | yes | 58 | yes |
| 7 | yes | 33 | yes | 59 | yes |
| 8 | yes | 34 | no | 60 | no |
| 9 | yes | 35 | yes | 61 | yes |
| 10 | yes | 36 | yes | 62 | yes |
| 11 | no | 37 | yes | 63 | yes |
| 12 | yes | 38 | yes | 64 | no |
| 13 | yes | 39 | yes | 65 | no |
| 14 | yes | 40 | yes | 66 | yes |
| 15 | no | 41 | yes | 67 | no |
| 16 | no | 42 | yes | 68 | yes |
| 17 | yes | 43 | yes | 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 | no | 73 | no |
| 22 | yes | 48 | yes | 74 | yes |
| 23 | no | 49 | yes | 75 | Not Answered |
| 24 | no | 50 | yes | 76 | yes |
| 25 | Not Answered | 51 | yes | 77 | yes |
| 26 | yes | 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 | 525 |
|---|---|

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • You had the best asset inventory of the all the teams i have judged. I really liked the layout and how you listed the ports and the services together.<br>• Great summary of the network!<br>• Very well done on the asset inventory<br>• Thank you for providing a comprehensive overview of the system, as well as using terminology suitable for leadership discussions.<br>• The entry excels in presenting a comprehensive and detailed assessment of the IT infrastructure and vulnerabilities, showcasing a robust understanding of both the technical and security aspects of the system. The clear documentation of asset inventory, network diagram, identified vulnerabilities, and corresponding mitigations demonstrates a systematic approach to risk identification and remediation. Moreover, the use of advanced tools like Sysinternals Suite, Linpeas, and Process Explorer highlights a sophisticated methodology for vulnerability scanning and system hardening. | • more detail on the vulnerabilities and the mitigation<br>• There needs more work done on the network diagram<br>• Expand on making sure that the hardening steps is an overall view and then proper justification is made for all.<br>• Hardening should be the steps you take, along with justifications, no improving the security posture of the system, not a rehash of you found vulnerabilities and patched them.<br>• I suggest incorporating the router icon and lines to enhance visual connectivity among all devices within the network.<br>• The vulnerabilities could be prioritized based on their severity or potential impact on the organization's operations. Categorizing them as critical, high, medium, or low risks would help in resource allocation and action planning.The entry could include suggestions for long-term security strategies, such as implementing automated monitoring tools, periodic penetration testing, or adopting a zero-trust architecture. This forward-looking perspective would add strategic value. Including a brief discussion on the potential impact of unresolved vulnerabilities on operations, reputation, and compliance would underscore the importance of the mitigations. |

### 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 | 505 |
|---|---|

| *Strong Points* | *Areas of Improvement* |
|---|---|

| | |
|---|---|
| • The presentation itself was put together really nicely - no large blocks of text or distracting graphics.<br>• I like that you had a timeline and cost associated with the strategies.<br>• Good ideas for strategy and priority<br>• A strong point of this entry was its structured approach in addressing each stage of the cybersecurity breach response, with a clear focus on risk assessment, incident containment, and recommendations for future prevention. The use of a detailed week-by-week recovery timeline demonstrates a proactive strategy and gives clear steps for immediate and long-term actions. This clarity helps to build confidence in the team's preparedness and thorough planning. | • I think it's important that presentations be rehearsed before you go in front of your audience - there was really only 1 presenter for the bulk of the presentation and he was standing in front of the screen obstructing the presentation during the entire recording. I also think a second look at the remediation timeline would be appropriate - I'm not sure that 4 weeks is sufficient to conduct a full scale forensic analysis of a cyber security breach to a power company, especially if you need to prepare a report and present the results to your government clients as well as the C-Suite.<br>• I think the presentation could have been better prepared. Also, the presenter was in front of the screen, blocking part of the slides. I would have liked more detail and not as many pauses. The dress code was not followed.<br>• Blocking the screen with their body. Cost estimates are very under estimated<br>• Ensuring more polished language, such as avoiding informal phrases like "various clients and whatnot," would strengthen the team's credibility.The "Annual Cost Summary" section could benefit from more detailed explanations of the specific services or software to be implemented. This would help the leadership team understand both the justification and the practicalities of the investment. Overall, focusing on language refinement, adding specific details, and strengthening the rationale for each recommendation would make this entry more comprehensive and professional. |

## 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 | 50 | 25 | 50 | 50 | 50 | 75 | 50 | 25 | 100 |

| Whack a Mole | |
|---|---|
| WAM1 | WAM2 |
| 0 | 281 |

### 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 |
|---|---|
| 1565 | 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 |
|---|
| 1413 |