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

# TENNESSEE TECHNOLOGICAL UNIVERSITY

## CYBEREAGLES

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 24 SCORECARD

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

| Score Category | Team Points | Percent of Points | Team Ranking |
|---|---|---|---|
| Anomalies | 1301 | 65.05% | 6 |
| Security Documentation | 979 | 97.90% | 3 |
| C-Suite Panel | 831 | 83.10% | 50 |
| Red Team | 2175 | 87.00% | 1 |
| Blue Team | 2000 | 100.00% | 1 |
| Green Team Surveys | 1482 | 98.80% | 2 |
| *Deductions* | 0 | | |
| Overall | **8768** | **87.68%** | **2** |

## 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 | 1301 |
|---|---|

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 | yes | 55 | yes |
| 4 | yes | 30 | yes | 56 | yes |
| 5 | yes | 31 | yes | 57 | yes |
| 6 | yes | 32 | no | 58 | yes |
| 7 | yes | 33 | yes | 59 | yes |
| 8 | yes | 34 | no | 60 | yes |
| 9 | yes | 35 | no | 61 | yes |
| 10 | yes | 36 | yes | 62 | yes |
| 11 | no | 37 | no | 63 | yes |
| 12 | yes | 38 | yes | 64 | yes |
| 13 | yes | 39 | yes | 65 | no |
| 14 | yes | 40 | yes | 66 | yes |
| 15 | yes | 41 | yes | 67 | Not Answered |
| 16 | no | 42 | Not Answered | 68 | yes |
| 17 | yes | 43 | no | 69 | Not Answered |
| 18 | yes | 44 | yes | 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 | yes | 75 | yes |
| 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 | 979 |
|---|---|

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • Overall excellent submission!<br>• Excellent work overall, with a thorough asset inventory, comprehensive port scan, a system overview tailored for senior leadership, and a clear, well-organized network diagram<br>• Good list of assets and vulnerabilities.<br>• Lots of vulnerabilites identified; strong diagram with clear legend. | • Could have included a little more business justification on the System overview.<br>• The identified vulnerabilities could be made more comprehensive to ensure a thorough assessment.<br>• I wanted more thought and detail into the system hardening and system overview.<br>• Although system hardening steps were reasonable and justified, there was little explanation on why the vulnerabilites were important to mitigate. |

### 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 mention of future risks<br>• Full notes in next answer. lots of great suggestions for reducing risk.<br>• Spoke confidently and directly to the audience (camera) with professional supporting slides.<br>• Great presentation and good points that you addressed | • No mention of system hardening<br>• PRESENTATION - 4/4<br>• full points you did all the things<br>• BUSINESS CONCERN RISKS - 2/4<br>• Would like to see concrete numbers<br>• No specific discussion of how degraded energy output leads to negative outcomes beyond "we failed to provide the service we promised, causing reputational damage"<br>• No mention of AoR<br>• Minimal jargon<br>• RISK REDUCTION STRATEGY - 3/4<br>• "long term" means years fyi<br>• +1 for customer feedback form. no discussion of what, if any, responses will be made however<br>• +1 for cyber insurance. 4 weeks is optimistic for legal review, however. also, how is failover redundancy connected to insurance? and how do you intend to do |

| | |
|---|---|
| | it? and it definitely takes a lot longer than 4 weeks<br>• compliance management is an ongoing process, and would need something more specific than "have a team and do it" to get the point. examples: discuss how compliance with NERC CIP also helps provide security, discuss specific measures to improve compliance with one specific regulatory standard such as CIP-010, discuss why it is necessary to devote separate resources from existing compliance department<br>• RECS -<br>• HIGH PRIORITY RECOMMENDATIONS - 2/4<br>• Update and Patch - yes, you need to do this at the start, and you need to do it regularly moving forward. even if you're just trying to do it once, patching an entire enterprise network in 3 days is optimistic, I'd typically expect a few weeks.<br>• +1 for security insight tooling through Wazuh, although I would expect maybe a few months minimum to deploy an asset like that<br>• Network Segmentation -<br>• missed opportunity to discuss airgap. what is the critical energy network, what is in it, how is it securely accessed<br>• pfsense software is free but it requires hardware to run it on. even if you're running it as a tenant in an existing virtualization farm (not ideal, give firewalls dedicated hardware ESP for OT airgaps), this takes a modern CPU, at least two dedicated network cards, and non-negligible RAM. Wazuh is also not free but wanted to give you the point there.<br>• FUTURE RISKS<br>• "Catastrophic" is a very powerful word. The way you're using this, the C-Suite is immediately going to ask what you're doing to prevent ransomware. Furthermore, what are the "company systems" that you are most concerned with protecting?<br>• QUALITY - 4/4<br>• OVERALL - lots of great suggestions for reducing risk; however, high priority recommendations felt overly optimistic. also would have appreciated greater detail |

| | |
|---|---|
| | of risks specifically due to degraded energy output<br>• Risk reduction strategies could have more directly addressed the identified business risk (ex: what strategy reduces the identified risk of lawsuits)<br>• expand more on your high priority recommendations |

## 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 |
| 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 75 | 100 |

| Whack a Mole | |
|---|---|
| WAM1 | WAM2 |
| 375 | 375 |

### 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 |
|---|---|
| 1600 | 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 |
| --- |
| 1482 |