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

# CALIFORNIA STATE UNIVERSITY-SAN BERNARDINO

## Y0TI3 H4CK3$

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 95 SCORECARD

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

| Score Category | Team Points | Percent of Points | Team Ranking |
|---|---|---|---|
| Anomalies | 200 | 10.00% | 90 |
| Security Documentation | 645 | 64.50% | 73 |
| C-Suite Panel | 768 | 76.80% | 67 |
| Red Team | 1156 | 46.24% | 54 |
| Blue Team | 1704 | 85.20% | 68 |
| Green Team Surveys | 1390 | 92.67% | 56 |
| *Deductions* | 0 | | |
| Overall | **5863** | **58.63%** | **56** |

## 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 | 200 |
|---|---|

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

| | | | | | |
|---|---|---|---|---|---|
| 1 | yes | 27 | Not Answered | 53 | no |
| 2 | yes | 28 | no | 54 | Not Answered |
| 3 | yes | 29 | no | 55 | yes |
| 4 | yes | 30 | no | 56 | no |
| 5 | yes | 31 | Not Answered | 57 | yes |
| 6 | yes | 32 | Not Answered | 58 | yes |
| 7 | yes | 33 | Not Answered | 59 | yes |
| 8 | yes | 34 | no | 60 | yes |
| 9 | yes | 35 | Not Answered | 61 | yes |
| 10 | yes | 36 | Not Answered | 62 | yes |
| 11 | Not Answered | 37 | yes | 63 | yes |
| 12 | Not Answered | 38 | Not Answered | 64 | Not Answered |
| 13 | Not Answered | 39 | Not Answered | 65 | Not Answered |
| 14 | yes | 40 | Not Answered | 66 | no |
| 15 | no | 41 | Not Answered | 67 | Not Answered |
| 16 | Not Answered | 42 | Not Answered | 68 | Not Answered |
| 17 | Not Answered | 43 | Not Answered | 69 | Not Answered |
| 18 | Not Answered | 44 | Not Answered | 70 | Not Answered |
| 19 | Not Answered | 45 | Not Answered | 71 | Not Answered |
| 20 | Not Answered | 46 | Not Answered | 72 | Not Answered |
| 21 | Not Answered | 47 | Not Answered | 73 | Not Answered |
| 22 | yes | 48 | Not Answered | 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 | 645 |
|---|---|

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • The system overview was clear and written with senior leadership in mind.<br>• The network diagram was very clear and straightforward.<br>• Got most of the key points of the network documented.<br>• System overview was an excellent summary of the system and how it operates, well written for a C-Suite/Non-technical audience. | • The vulnerability list could be expanded upon. Formatting needed some attention too, blank spaces, fonts, general consistency throughout.<br>• There are many vulnerabiltities within the system. Try to be more thorough in your internal investigation.<br>• Ensure there is consistency throughout the document.<br>• Known vulnerabilities missed many of the obvious vulnerabilities that were easily discoverable upon logging into the machines. Most results appeared to be solely from a vulnerability scan. |

### 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 | 768 |
|---|---|

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • Everything was professional and explained.<br>• Nice, professional slides and overall flow of presentation.<br>• The thorough explanation and reasoning behind the proposed improvements for each phase were well articulated. The case study of the recent breach of PG&E was a nice addition to the presentation as to why it is important.<br>• The actions in the phases are thoroughly planned. | • Mixing up of the strategy to reduce risk and the high priority risks together in a way.<br>• Very short section/discussion of business risks.<br>• no comment<br>• One has to interpret what your long-term strategy is, and what your immediate recommendations are. Try to adhere to the prompt and clearly answer the questions in the brief. |

## 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 | 100 | 50 | 75 | 25 | 25 | 100 | 0 | 0 | 50 |

| Whack a Mole | |
|---|---|
| WAM1 | WAM2 |
| 281 | 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 |
|---|---|
| 1600 | 104 |

## 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 |
|---|
| 1390 |