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

SCORECARD WITH COMMENTS

ILLINOIS STATE UNIVERISTY – TEAM # 82

Total Score	6611

BLUE TEAM SCORING

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
1968

RED TEAM SCORING

ASSUME BREACH

This year we will be using **ASSUME BREACH** for part of your Red team score. This will be worth 1500 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.

Assume Breach								
Attack Chain 1	*Attack Chain 2*	*Attack Chain 3*	*Attack Chain 4*	*Attack Chain 5*	*Attack Chain 6*	*Attack Chain 7*	*Attack Chain 8*	*Attack Chain 9*
0	120	90	90	60				

EXTERNAL PENTESTING (TRADITIONAL)

This portion of the Red team score will be worth 1000 POINTS. This will be done via an automated scripted check.

External Pentesting
652

GREEN TEAM SCORING

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	Comments:
930	• I erroneously registered Team 82 as Team 79 Hopefully you can remove my Team 79 eval • Admin login worked, but admin page was not implemented as of 12:18pm ET • Great job, almost there! Good luck! • Yes No data on the Home page

ORANGE TEAM SCORING

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	Strong Points:
878	• Nice asset inventory table and network diagram. Nicely formatted and detailed. • Asset inventory listing of port/service details is above and beyond **Areas of Improvement:** • Remove template instructions. • System Overview is lacking any notification to senior leadership that all the systems have vulnerabilities.

C-SUITE PANEL BRIEF

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	Strong Points:
853	• Thank you for identifying that company culture and employee morale is an immediate risk during mergers and acquisitions, that cannot be mitigated immediately but takes a longer term plan and solution to address. • Recognized work culture clashes as a potential risk. • Nice and concise breakdown of both immediate and long term plans • Good flow and good presentation. **Areas of Improvement:** • Tie your long term recommendations back to the risks you identified as having a long term solution. Awareness training, IDS,

	and 3rd party cybersecurity audit don't specifically address culture and morale. • Immediate action item to use open-source software to secure devices should discuss the specific problem that is being addressed. Are you talking about host AV, a container security solution, database audit software, configuration management software, a ne • Provide clarity if this was only a 2 person team; nice presentation • One suggestion for short term would be to keep Sole's network isloated from the main networks until vulnerabilities and the breech have been mitigated

ANOMALY SCORING

Anomalies simulate the real-world challenges that cybersecurity professionals face daily in the industry. Anomalies are mapped the NIST NICE Framework, and fall into one of seven categories: *Analyze, Collect and Operate, Investigate, Operate and Maintain, Oversee and Govern, Protect and Defend, and Securely Provision*. Anomalies are also mapped to a knowledge, skill, ability, and task role within each category.

Anomaly Score
970