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

PURDUE UNIVERSITY NORTHWEST

PNW ROAR

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 69 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	712	35.60%	37
Security Documentation	782	78.20%	60
C-Suite Panel	661	66.10%	81
Red Team	794	31.76%	74
Blue Team	1985	99.25%	36
Green Team Surveys	128	8.53%	72
Deductions	0		
Overall	**5062**	**50.62%**	**72**

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	712

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

1	yes
2	yes
3	yes
4	yes
5	yes
6	yes
7	yes
8	yes
9	no
10	yes
11	no
12	no
13	yes
14	yes
15	yes
16	no
17	yes
18	yes
19	yes
20	yes
21	yes
22	yes
23	yes
24	no
25	Not Answered
26	Not Answered
27	Not Answered
28	Not Answered
29	Not Answered
30	Not Answered
31	Not Answered
32	Not Answered
33	Not Answered
34	Not Answered
35	Not Answered
36	yes
37	yes
38	Not Answered
39	Not Answered
40	yes
41	yes
42	Not Answered
43	Not Answered
44	Not Answered
45	no
46	yes
47	yes
48	yes
49	no
50	yes
51	yes
52	yes
53	Not Answered
54	yes
55	yes
56	no
57	yes
58	yes
59	yes
60	yes
61	Not Answered
62	yes
63	yes
64	yes
65	Not Answered
66	Not Answered
67	Not Answered
68	Not Answered
69	Not Answered
70	Not Answered
71	Not Answered
72	Not Answered
73	Not Answered
74	Not Answered
75	Not Answered
76	yes
77	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	782

Strong Points	*Areas of Improvement*
• Network Diagram and Vulnerability report were excellent! • You have a good foundation started. • Known vulnerabilities section was well done. • All assets listed; appropriate mitigations for vulnerabilities	• System Overview and Asset Inventory needed a bit more work. • With more detailed discovery and documentation of you network you would increase your scores for vulnerabilities and system hardening. • The system hardening section presents an opportunity for improvement in several areas, including the need for comprehensive and technically sound hardening steps. It is essential to provide strong justifications for the decisions made by the team, whether in actions taken or not taken. Additionally, open-source tools should be listed. • +1 hardening step with more overall justification; language in system overview and hardening should be more targeted/professional for senior leadership

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	661

Strong Points	*Areas of Improvement*
• Good long term ideas • Recommendation of opensource tools and addressing staffing issues that is slowing the network mapping. • Full notes in next answer. You have a good understanding of the problem and possible solutions. • Active participation from both presenters. Smooth and meaningful transition between topics.	• Nmap and Forensics are not good priorities during a crisis • Presentation was very short, you had some good information that could be expanded upon. Also, strongly consider using visual aids or slides in your presentation. A few slides with some key points related to your discussion can go a long way. Roughly 30% of adults are auditory, about 65% are visual, whenever possible deliver a presentation that accounts for both. When briefing the C-Suite you are expected to

	put in the extra effort, the little things matter. • REQUIRED ELEMENTS - 2/4 • video is 2min39s • two presenters • RISKS TO CORE BUSINESS 2/4 • how would degraded energy output impact gov facilities? no specifics given • a company can continue to meet its core mission even with unaddressed risks - most do, it's terrifying. furthermore, the response to risk in many cases is simply to purchase insurance appropriate for that risk. as an OT professional, my job is not to eliminate risk but to properly mitigate it. • STRATEGY TO REDUCE RISKS 3/4 • prioritizing gov facilities for restoration in case of disruption, prioritizing systems for "production and distribution" of energy +1 • production is Generation, distribution is Transmission and Distribution. read up on difference between T&D, very important • could have gained an another point for "prioritizing systems for production and distribution" on its own, if you had discussed some of these systems (ICS/SCADA, Purdue levels 3 and below, etc). I understand that you have specifically not been given technical network details, but it's reasonable and practical to assume that any given OT network you encounter is going to share certain high level characteristics such as some manner of ICS/SCADA/DCS/etc, enterprise server racks talking to specialized field devices over protocols such as Modbus or DNP3, HMIs, data historians, etc) • +1 for elasticsearch recommendation as SIEM • HIGH PRIORITY RECOMMENDATIONS • interesting approach of "train up your existing employees to do networking work as well", plus recommendation of using nmap as port mapping tool +1 • i don't think this is a very realistic recommendation, but that doesn't mean it doesn't mean the rubric requirements. i understand the desire for low/no cost solutions, but employees are already going

	to have full time requirements and are going to be hostile to the idea of taking on additional responsibilities that they are not adequately trained for. • in any given OT org, there's gonna be at least one person who is responsible for making networking work. i would thus reframe your suggestion as "have networking begin conducting regular nmap scans and make the results available to all of IT. have SMEs understand which ports are necessary for assets they administer and close unnecessary services where possible". this way, only networking employees are asked to do specifically networking tasks, and all other IT employees are only asked to develop a deeper understanding of the assets they already administer. • digital forensics is a good suggestion, no tools given, also requires incredibly specialized skillset and 95% of OT orgs are going to contract that out to Mandiant or Dragos, and neither is cheap • communications to rest of org is good, no tools given • QUALITY - 1/4 • no slides or visual aids • OVERALL - you are missing several items from the rubric, but your understanding of the problem and potential solutions is good. • Length requirement was not fulfilled. Use pauses and change of inflection to emphasize the most important information. Recommendation funding, justification, and future impacts could be highlighted more clearly.

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	0	100	25	0	25	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
1585	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
128