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

LOUISIANA STATE UNIVERSITY

LSU TIGERS

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 55 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	929	46.45%	18
Security Documentation	805	80.50%	57
C-Suite Panel	881	88.10%	30
Red Team	894	35.76%	70
Blue Team	1995	99.75%	26
Green Team Surveys	1479	98.60%	33
Deductions	0		
Overall	**6983**	**69.83%**	**33**

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	929

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

1	yes	27	no	53	no
2	yes	28	Not Answered	54	yes
3	yes	29	Not Answered	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	Not Answered	60	yes
9	yes	35	Not Answered	61	yes
10	yes	36	yes	62	yes
11	no	37	no	63	yes
12	yes	38	no	64	no
13	yes	39	yes	65	no
14	yes	40	yes	66	Not Answered
15	yes	41	no	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	yes	43	Not Answered	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	yes
22	yes	48	yes	74	yes
23	yes	49	yes	75	Not Answered
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	805

Strong Points	*Areas of Improvement*
• System hardening was written in a way that was easy to follow. • Nice job on the vulnerability identification and mitigation write up. • Your system overview is good. • Good System Hardening section. This topic always has the potential to be difficult to explain to a non-technical audience, however it was very clear and easy to read for a non- technical audience • The asset information was very thorough, however a brief explanation of why components had multiple IP addresses would be helpful to the non-technical audience •	• MapBox was missing from both the inventory and diagram. • A little more attention to detail - missed the Map Box for both the asset and network diagram. • Your system inventory and network diagram are missing the "map box." • In the System Overview, It may be helpful to the audience to give a “big picture” of the System being reported on. The information was technically correct. • The Vulnerability Table was exceptional and easy for a non-technical audience like upper management. There where some grammar mistakes in the table that may reduce some of the professional polish that this report shows in abundance

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	881

Strong Points	*Areas of Improvement*
• I liked how you addressed each area of the CIA triad without actually referencing the triad. You were to the point and delivered important CIA related information without the distraction of explaining the triad and why its important. I felt that same efficiency throughout the presentation, not rushed and to the point. I felt well informed and confident in	• So its clear, I want you to have fun with this competition, this more an observation than an improvement. That said, really consider the use of emojis in your presentations. A C-Suite dealing with a cyber breach will likely have someone who wont like the frowny face and thumbs down. Its a small detail, but you dont want to give anyone the impression that you aren't taking the event seriously because they wont take your recommendations seriously. • The detail on each slide was sparse and could have had more detail and a bigger font for legibility. • More clarity of relating strategies to business risks • REQUIRED ELEMENTS - 4/4 • RISKS TO CORE BUSINESS - 3/4 • Would like to see specific figures (case studies are good for when you don't have specifics of your org) • Good analysis of risks of degraded energy output

your recommendations, really well done! • Graphic on the slides were nice and the presentation was professional. • Nice visualizations and representation of business risks • Full notes in next answer.	• Minimal jargon • HIGH PRIORITY RECOMMENDATIONS - 2/4 • Logging is good, but will have you SIEM or store locally? what logs? (e.g. Windows has 5 or 6 event logs, most people use just SYSTEM and SECURITY) any specific tools? syslog is better understood as a data format rather than a tool; it's built into Linux by design and Windows is technically capable of it. also, even if you use strictly FOSS tools like Elastic Stack or Security Onion, will require substantial spend on workers • Password Policy is a decent rec, but I want to focus on MFA, which is an EXCELLENT rec, but a) very hard to do in 2 weeks, you're talking plugging a new step into every single critical login process, doing it sloppily is worse than not doing it at all if it breeds a false sense of security while non-MFA auth paths still exist. also, what tool? free MFA solutions such as SMS or email based are easily bypassed by attackers, and most experts recommend companies with dedicated apps such as Duo, or hardware tokens like RSA/Yubikey, neither of which is free. • Network Hygiene (+1 point) - "only necessary ports in the business network" this is a great opportunity to discuss, what is the business/enterprise/IT network and what is the OT network, and what network hygiene measures (airgap cough cough) can take advantage of this natural division of assets. wireshark and nmap are good tools for gathering data, but where/how are you gonna store the results and access them later? there are a lot of answers here from "Google Sheets" to "SCADA ITSM database solution", no single right answer so long as your arguments are strong • "we will also be setting up auto-updating for our organization's software" this is very very dangerous for an enterprise, ESPECIALLY one that handles critical physical processes such as Energia Ventosa. remember the crowdstrike outage a couple months back? imagine if your electric utility auto-installed Microsoft updates on their SCADA servers. not docking any points, just wanted to call attention to this specifically • Encryption - need more details/discussion for the point. Data at rest, in transit? How are keys stored? What tools? This is even a great opportunity to start talking about post-quantum crypto, given that Chinese researchers now claim to have broken 22-bit RSA on a commodity quantum machine - https://www.livescience.com/technology/computing/chinese-scientists-claim-they-broke-rsa-encryption-with-a-quantum-computer-but-theres-a-catch. • STRATEGY TO REDUCE RISKS - 2/4 • +1 cybersecurity training. • network segmentation and SIEM are both strong recommendations, but neither was really adequately explored for those to also gain points. • no direct connection back to risks

	• QUALITY - 4/4 • OVERALL - high priority recommendation analysis was good, would have liked to see much more discussion of long-term risk reduction strategy as well. these two items are connected, but if you don't specifically make the connection between say, logging as a HPR and implementing a SIEM as part of your long term strategy, C-Suite types who already have a million financial/operational/regulatory/external concerns are not going to make that connection in the 5 minutes you have with them.

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	75	25	50	0	0	50	0	50

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
1595	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
1479