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

LOYOLA UNIVERSITY CHICAGO

LOYOLA UNIVERSITY CHICAGO

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 54 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	637	31.85%	51
Security Documentation	956	95.60%	10
C-Suite Panel	767	76.70%	68
Red Team	1850	74.00%	14
Blue Team	1980	99.00%	38
Green Team Surveys	1493	99.53%	14
Deductions	0		
Overall	**7683**	**76.83%**	**14**

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	637

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

1	yes		27	no		53	yes
2	yes		28	no		54	Not Answered
3	yes		29	Not Answered		55	yes
4	yes		30	no		56	yes
5	yes		31	no		57	yes
6	yes		32	Not Answered		58	yes
7	yes		33	Not Answered		59	yes
8	yes		34	yes		60	no
9	yes		35	Not Answered		61	yes
10	yes		36	yes		62	yes
11	no		37	yes		63	yes
12	Not Answered		38	yes		64	no
13	yes		39	yes		65	Not Answered
14	yes		40	yes		66	no
15	yes		41	Not Answered		67	Not Answered
16	yes		42	Not Answered		68	Not Answered
17	yes		43	Not Answered		69	no
18	yes		44	Not Answered		70	yes
19	yes		45	Not Answered		71	yes
20	Not Answered		46	Not Answered		72	yes
21	yes		47	Not Answered		73	Not Answered
22	yes		48	Not Answered		74	yes
23	Not Answered		49	Not Answered		75	yes
24	yes		50	Not Answered		76	yes
25	Not Answered		51	Not Answered		77	yes
26	no		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	956

Strong Points	*Areas of Improvement*
• Vulnerabilities was really well done. The executive summary was a nice addition for helping senior leadership understand. Adding a severity column was also helpful, easy way to visualize the findings for senior leadership. • Really nice job on the vulnerabilities - including e.g. the severity of each. • Your formatting and sorting of the vulnerabilities table is excellent, as is the content! • The entire report was exceptionally well-written and professional • Having an executive summary in the vulnerabilities section seemed to show a Vulnerability Management Plan • The severity of the vulnerability table used the recognized "risk assessment"colors which made it easier to prioritize mitigations.	• Be sure your asset inventory and network diagram are consistent. MapBox was in your diagram but missing on the inventory. • More attention to detail is needed (missed the Map Box in the asset section). • Your system inventory did not list the map box, yet your network diagram does. • No comments here

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	767

Strong Points	*Areas of Improvement*
• Appreciate that three out of four team members presented and the presentation was very professional. • Clear, strategies laid out • Full notes in next answer, but High Priority Recommendations section was excellent • Strong high-priority recommendations	• The action items were a little too in the weeds for C-suite and the slides could have used some graphics. • Better distinction of high priority items and tie in to financial risks • REQUIRED ELEMENTS - 4/4 • be sure to include your team number within the video, and present full names and roles for each participant (Security Team Member is sufficient for this exercise) • RISKS TO CORE BUSINESS - 3/4

	• risks are well posed, consider data centers in AoR, concerned primarily with business bottom line • minimal jargon • would have liked to see further examination of risk due specifically to degraded energy output • no specific figures given • STRATEGY TO REDUCE RISKS - 1/4 • No specific measures given; I thought that the next section was your long-term strategy at first, and some of the items, esp compliance with a new framework, are definitely not achievable in the short-term. however, i will give you the full 4/4 that i was prepared to give you when I thought that that was your strategy section, as your suggestions and analysis are otherwise consistently excellent throughout that section • HIGH PRIORITY RECOMMENDATIONS - 4/4 • you say that Energia Ventosa is 'uniquely vulnerable to attack' due to high number of gov customers. you might be trying to say 'unique risk from attack', uniquely vulnerable implies to me that you're concerned about EV getting popped through a supply chain breach of one of those customers. a valid concern but not what i think you're trying to get at here • phishing training - good callout for 'report phish' button, good callout for need for regular training. would have liked to see a specific open source tool highlighted, but i'll give you the point because you also called out 'no undue burden on employees', very very important consideration +1 • Excellent analysis of needs to implement NIST CSF 2.0 +1. The most common/relevant cybersecurity regulations for energy companies are the NERC CIP standards, but EV would almost certainly already have a well-staffed NERC CIP team, so NIST CSF is a great opportunity to explore a suggestion they most likely have not implemented. • Consistent client communication - this does cost money, whether it's the workers who handle the comms, the need to update the company website for the first

	time since 2003, etc. however, the rest of your analysis is good enough to earn the point. +1 • QUALITY - 4/4 • OVERALL - excellent high priority recommendations section! if you had the opportunity to do this over again, i would recommend taking that list and evaluating your suggestions as short-term/tactical vs long-term/strategic in order to determine what could be Risk Reduction Strategy and what could be High Priority Recommendations. • The long-term strategy should consist of three or more long-term actions. These are different from three to four immediate actions/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 point*s. 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	0	75	100	100	50	0	50	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
1580	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
1493