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

AUBURN UNIVERSITY

BUFFEROVERFLOW

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 9 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	813	40.65%	27
Security Documentation	915	91.50%	23
C-Suite Panel	905	90.50%	19
Red Team	1606	64.24%	26
Blue Team	1980	99.00%	38
Green Team Surveys	1413	94.20%	15
Deductions	0		
Overall	**7632**	**76.32%**	**15**

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	813

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

1	yes		27	no		53	yes
2	yes		28	yes		54	Not Answered
3	yes		29	no		55	no
4	yes		30	Not Answered		56	no
5	no		31	no		57	yes
6	yes		32	Not Answered		58	yes
7	yes		33	Not Answered		59	yes
8	yes		34	no		60	no
9	yes		35	Not Answered		61	yes
10	no		36	yes		62	yes
11	yes		37	yes		63	yes
12	Not Answered		38	no		64	yes
13	yes		39	yes		65	no
14	no		40	yes		66	Not Answered
15	yes		41	no		67	Not Answered
16	yes		42	Not Answered		68	Not Answered
17	yes		43	no		69	Not Answered
18	no		44	yes		70	yes
19	no		45	no		71	yes
20	no		46	yes		72	yes
21	no		47	no		73	no
22	yes		48	yes		74	yes
23	yes		49	yes		75	Not Answered
24	no		50	yes		76	yes
25	no		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	915

Strong Points	*Areas of Improvement*
• A strength of this entry was the network diagram. It contained a strong foundation of knowledge and presented the architecture in a professional, descriptive manner. Well done. • Well detailed technical explanations • In the system overview you explained most acronyms, good job explaining systems and functionality, vulnerabilities, well formatted & easy to read, mitigations listed using minimal jargon and easy to understand, broken out by machine, scan info listed then hardening steps taken, very professional, appreciate using close to full word count • The team went in-depth with system hardening, the diagram was easy to read, and all the hosts were listed.	• An improvement for this submission would have been to identify additional vulnerabilities. In this scenario, 30+ list entries is feasible. 23 is good, but too many went undetected. • System overview could be improved with an executive summary. Asset inventory missing the MapBox • the system overview got a little into the weeds listing port numbers instead of what they were protecting against and tools instead of what the tools did, • The diagram included a key but used identical symbols for servers and PCs, which caused confusion. Additionally, the System Overview could have been framed more higher level, using terms more accessible to C-suite personnel.

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	905

Strong Points	*Areas of Improvement*
• Nice job connecting strategy to previous risks • This team was excellent and well prepared. They checked every box. • The presenters were well prepared for this submission it did not seem like script but more like things came naturally to all members. great work on putting this together and loved the recommendations with cost part as well. • Great job with overall presentation skills and crafting a narrative to be able to present. I felt like you all were able to do a great job communicating!	• Reasoning for recommendations is incomplete • Excellent work. Your team was ready and well prepared. Your video length was on point, every box was checked for me. Congratulations on job well done. You are on the right track, keep up the good work • I think one of the members was missing in the presentation. This could have been exemplary if all members were in there. • Three of the recommendations provided were at tremendous cost to the company ($8,500 estimated/month) which takes away from the speed they can be implemented at and overall the value.

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
100	50	50	50	50	0	75	0	50	75

Whack a Mole	
WAM1	WAM2
375	281

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
1413