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

BRIGHAM YOUNG UNIVERSITY

BYU 2

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 40 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	612	30.60%	54
Security Documentation	513	51.30%	81
C-Suite Panel	781	78.10%	64
Red Team	1375	55.00%	40
Blue Team	1985	99.25%	36
Green Team Surveys	115	7.67%	70
Deductions	150		
Overall	**5231**	**52.31%**	**70**

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	612

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	yes
10	yes
11	no
12	no
13	yes
14	yes
15	yes
16	yes
17	yes
18	yes
19	no
20	no
21	yes
22	yes
23	no
24	no
25	no
26	Not Answered
27	Not Answered
28	yes
29	Not Answered
30	Not Answered
31	Not Answered
32	Not Answered
33	Not Answered
34	Not Answered
35	Not Answered
36	no
37	yes
38	yes
39	no
40	no
41	Not Answered
42	Not Answered
43	no
44	yes
45	yes
46	Not Answered
47	Not Answered
48	Not Answered
49	yes
50	Not Answered
51	Not Answered
52	Not Answered
53	no
54	Not Answered
55	yes
56	no
57	yes
58	yes
59	yes
60	yes
61	yes
62	yes
63	yes
64	yes
65	Not Answered
66	Not Answered
67	Not Answered
68	Not Answered
69	Not Answered
70	yes
71	Not Answered
72	yes
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	513

Strong Points	*Areas of Improvement*
• Your goal at the end of the system overview was well placed. Even if senior leadership glazes over this section the last sentence likely catches there attention . • The system hardening section was understandable regardless of existing cyber knowledge. • The information was well organized, which made it easy to read. The system overview is well-defined, specifying both the system and its purpose in clear, plain language, which targets a senior leadership audience. The overview addresses the system's significance, components, and security practices thoroughly.	• Formatting, remove the instructions and examples so this looks more like report to leadership rather than an assignment. • Documenting all assets in the inventory and including firewall and internet in network diagram. Removal of instructions provided in template. • The network diagram includes several hosts but lacks key components and needs more technical soundness in logical connections. It does not meet the requirement for completeness and appropriate symbols for a proficient or exemplary level.

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	781

Strong Points	*Areas of Improvement*
• There were good low level descriptions and good tie in to beginning points and financials. • Only two active members - no acknowledgement of any other team members, strategy and recommendations need more clarity and integration of reasoning, • Strong focus on the importance of communication within an organization • Tied risks to financial concerns, such as fines, loss of customers, and operational costs.	• The camera angle was awkward and there was no acknowledgement of other team members. • Clear explanations avoided jargon. • No acknowledgement of other team members. • Visually distracting and unprofessional camera angle/background • Strategy addressed immediate risks, but the task was to provide long-term action items. • Provide more concrete estimates on cost and ROI. C-Suite will want hard number to justify implementation. • Consider showing slides during presentation, executives love PowerPoint.

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	75	50	25	0	50	50	50	100

Whack a Mole	
WAM1	WAM2
187	187

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
115