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

CALIFORNIA STATE POLYTECHNIC UNIVERSITY-POMONA

CAL POLY POMONA: WHAT'S A TERMINAL

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 13 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	587	29.35%	60
Security Documentation	925	92.50%	18
C-Suite Panel	837	83.70%	47
Red Team	1625	65.00%	24
Blue Team	1750	87.50%	65
Green Team Surveys	0	0.00%	57
Deductions	0		
Overall	**5724**	**57.24%**	**57**

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	587

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

1	yes	27	Not Answered	53	Not Answered
2	yes	28	no	54	Not Answered
3	yes	29	Not Answered	55	no
4	yes	30	Not Answered	56	no
5	yes	31	yes	57	yes
6	yes	32	yes	58	yes
7	yes	33	yes	59	yes
8	yes	34		60	no
9	yes	35		61	yes
10	yes	36	Not Answered	62	yes
11	no	37	yes	63	no
12	Not Answered	38	no	64	yes
13	yes	39	no	65	no
14	yes	40	no	66	Not Answered
15	no	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	yes	43	no	69	Not Answered
18	yes	44	Not Answered	70	no
19	Not Answered	45	no	71	yes
20	Not Answered	46	yes	72	yes
21	yes	47	Not Answered	73	Not Answered
22	Not Answered	48	yes	74	yes
23	no	49	Not Answered	75	Not Answered
24	no	50	yes	76	Not Answered
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	925

Strong Points	*Areas of Improvement*
• Nice job identifying and documenting the vulnerabilities and mitigations. • Excellent job! The system overview was detailed and to the point. The asset inventory matches the network diagram, which is clean and easy to read. Also, great job with system hardening it was detailed and you all listed the tools utilized for this project. • Very well written system overview and system hardening, including the overall impacts • Well done on the overview. Great job identifying the vulnerabilities. The hardening section was well explained, including each tool used.	• Needed a little more attention to detail; forgot one element from the asset and network diagram. • Nothing! Team 0013 did an exceptional job. • MapBox missing from Asset Inventory and Network Diagram • An asset was not identified in the asset list or the network diagram (mapbox).

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	837

Strong Points	*Areas of Improvement*
• High priority recommendations were great, excellent choices and overall a quality submission. • The slides are clean and the presentation was excellent. You've done a great job outlining the business risks—well done! • There was a visual appeal to the slides and it was done at a more professional level. • Security implementation cost compared to data breach was a nice addition. • Strategies to reduce risk were clear and logical.	• The risk reduction strategies slide was lacking; it would have been great to get better visuals and perhaps a bit more color on how you're planning to implement network encryption on OT networks. • You did a fantastic job highlighting the business risks. Adding a strategy to address these risks alongside technical controls would make it even stronger. Great work overall! • Strategy to reduce risks needs to discuss how it impacts the business financial side. • Presentation length was shorter than expected. • No focus for free/open source 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 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	75	25	0	50	75	50	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
1350	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
0