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

CALIFORNIA STATE POLYTECHNIC UNIVERSITY, POMONA

THE DOOBY GOOBIES

November 15, 2025

In-Person

Number of Teams	Max Team Points Received	Min Team Points Received	Mean Team Points Received	Total Points Possible
93	8,783	1,267	6,146.81	10,000

TEAM 85 SCORECARD

This table highlights the *team's* efforts for the 2025 CyberForce Competition®.

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	335	22.33%	69
Security Documentation	1121	89.68%	30
C-Suite Panel	1113	89.04%	13
Red Team	1250	50.00%	27
Blue Team	1475	73.75%	68
Green Team Surveys	1320	88.00%	40
Deductions	0		
Overall	**6614**	**66.14%**	**40**

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. This year, challenges were longer, and some required more than one person to answer, effectively requiring teams to evaluate risk versus reward.

Anomaly Score	335

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

1	Yes	10.7	Yes	17	Yes
2		10.8	Yes	18	Yes
3	No	10.9	No	19	Yes
4		11.1	Yes	20	Yes
5		11.2	Yes	21	No
6		11.3	Yes	22	
7	No	11.4		23	
8		11.5		24	
9	No	11.6		25	
10.1	Yes	11.7		26	
10.2	Yes	12		27.1	No
10.3	Yes	13	No	27.2	No
10.4	Yes	14		28	Yes
10.5	Yes	15	Yes	29	No
10.6	Yes	16	Yes	30	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	1121

Strong Points	*Areas of Improvement*
• Overall good documentation. • The team did a very good job of identifying system vulnerabilities and had a well-thought-out system hardening plan. • The report is clearly written and logically organized. The findings demonstrate good attention to host-level detail. Formatting is consistent, and the document reads professionally from start to finish. • Good hardening description. • Detailed yet simple enough language for senior executives	• I think the hardening part was the weakest part of the documentation, but it was still good. • To bring your report to the next level, I'd add more formatting to assist senior-level staff such as color-coded severity in vulnerabilities, grouping assets together in the asset inventory rather than a row for each service, etc. This is very nit-picky - good job! • Severity ratings should be added to the vulnerability section.

Strong Points	Areas of Improvement
	• Unresolved issues should include compensating controls, and a summary table of the top risks would help prioritize remediation." • Lacks logical connections in network diagram. • A few small mistakes on asset inventory

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	1113

Strong Points	Areas of Improvement
• Highly polished and professional. Presentation clearly integrates business continuity, legal, and technical with strong justification for each recommendation. • Excellent job tying recommendations back to risks explicitly and explaining how they will help. • Financial Focus and Risk Assessment (Risks Related to Operational and Business Concerns - 30%): The team provided a clear summary of risks suitable for all members of the C-Suite. Crucially, they clearly identified how risks affect the company's concerns and their bottom line (finances). They supported their assessment with specific industry figures, noting that unplanned offshore platform downtime averages around 3 million. This demonstrated a clear understanding of business impact. • Complete Strategy (Strategy to Reduce Risks - 30%): The team provided a complete strategy to reduce risk. This included immediate containment and recovery steps (network segmentation, internal audit, verified system backups), as well as listing three or more long-term action items. These long-term actions, such as implementing regular external security audits of third-party contractors and developing a comprehensive incident response plan which clearly addressed the identified business risks.	• Could have included implementation timeframes and manpower required for implementation and cost-benefit analysis for executive clarity and feasibility. • It was unclear how the "Internal" risks were related to the incident described. • Visual Aids and Professional Appearance: While slides were used, the entry lacked visual charts and calculations. To achieve the ""consistent, professional appearance"" expected for the C-Suite, especially when discussing significant financial impacts, the team should have graphically presented the financial data (e.g., the $38 million annual downtime cost or the $3 million incident cost). Visualizing these numbers on the slides would have enhanced the persuasive pitch and the overall quality of the briefing to a non-technical C-Suite audience. • Justification for Strategy Implementation: While the team's strategy was robust, incorporating more specific high-level discussion on elements like return on investment (ROI) or criticality for the strategy items would further strengthen the presentation's appeal to leadership, as suggested in the judging guidelines for high priority items. • Should state how the other associates contributed • May consider including more slides so that audience can reference the material on the slides. Slides were very minimal and the

Strong Points	*Areas of Improvement*
• Budget-Compliant and Justified Recommendations (High Priority Recommendations - 30%): Team 85 delivered 3-4 high priority actions that improved overall security and protected business continuity. They strictly adhered to the constraint that actions must require at most a minimal level of additional funding (e.g., use only free or open-source tools), specifically naming and justifying the use of OPNsense (Firewall), Velociraptor (EDR), and Ansible AWX (Automation). Complete and consistent reasoning was provided for all these actions, linking them directly to containment, eradication, and recovery. • Required Elements: The team successfully identified Team 85, included four active presenters, and provided clear acknowledgment of contributions from all six team members (including two associates), meeting the Exemplary requirement for participation • Nice use of embedded video over slides. • The financial impact slide was especially good, showing the difference in cost along with tools that are free. • Everyone presented well professionally and worked well off of each other.	audience may need touchpoints to reference from the slides that are not listed. • For high priority recommendations should include who will do the work, associated costs and timeline. Products may be open source but there will still be associated staffing costs, downtime costs, etc. • Long-term implementations should also be quantifies, what is the associated cost, staffing, software/hardware, and timelines. • Also recommend include references and prompting the audience to reach out with further questions. • In the future, I would recommend keeping one speaker per slide though this is a personal preference. Overall, great job! • When talking about the actions to take, put the tools and cost at the same time you are mentioning what needs to happen.

RED TEAM SCORING

RED TEAM FLAG INPUTS (ASSUME BREACH & WHACK A MOLE)

This year we will be using ***Assume Breach*** as part of your Red team score. This will be worth *1,750 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
125	125	125	125	125	0	125

Whack a Mole		
WAM1	WAM2	WAM3
250	125	125

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	ICS Score
1475	0

Each team was scanned *27 times* throughout the competition. Below identifies your team's number of successful service scans per required service. Each successful scan was awarded 5 points.

SMTP	IMAP	SMB (task)	NFS	SSH	HTTP	WinRM	LDAP	MariaDB	phpmyadmin	SMB (db)
27	27	27	26	27	26	27	27	27	27	27

The ICS Score was determined by the number of barrels you were able to produce during the competition. The max number of barrels a team should be able to produce (+/- slight variance) was 45,000 barrels. There were two periods in which minimal barrels, if any, should have been produced due to significant weather. The total number of points awarded was 515.

No. of Barrels Produced	Percentage of Total Barrels
0.00	0.00%

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
1320

Green Team Survey Comments
• Great job.
• Good Job!
• When on the Admin before the user management, there's a dashboard listed. (Please remove)
• Excellent work!
• 5:45 This site can't be reached
• This site can't be reachedweb.blue0085.cfc.local refused to connect.
• This site can't be reachedweb.blue0085.cfc.local refused to connect.