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

GOVERNORS STATE UNIVERSITY

JAGX

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 53 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	127	8.47%	92
Security Documentation	823	65.84%	82
C-Suite Panel	858	68.64%	83
Red Team	250	10.00%	82
Blue Team	512	25.60%	92
Green Team Surveys	0	0.00%	91
Deductions	0		
Overall	2570	25.70%	91

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	127

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

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

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	823

Strong Points	*Areas of Improvement*
• Overall, this was a very well written and organized report. • Overall, this is a technically solid and well-written document. It shows a strong understanding of both IT and OT systems, and it's clear that your team put real effort into mapping assets and explaining vulnerabilities. The way you handled the Samba misconfiguration on the Taskbox is excellent: it shows you understood the issue, knew why it mattered, and provided the exact steps to fix it. The vulnerability and hardening sections are detailed and	• The system hardening sections was way too detailed instead of giving a broad overview of what was done with justification for why mitigation steps were or were not taken. Cleaning this up and gearing it more towards senior leadership would elevate the entire report. • "There are a few places that need some cleanup before the report is fully finished. The technical content is excellent, it just needs that last round of checks to make sure it is ready. The document has a blank page and ends with a leftover template text,

Strong Points	Areas of Improvement
well written, with realistic actions and a consistent structure that makes it easy to follow. Overall, your technical accuracy and documentation quality are very good, and it shows that you know what you're doing. • The report is polished and detailed. The hardening section feels real and implementable. It names specific commands, policy settings, and expected outcomes. The writing is clean and confident, suitable for both technical staff and management. • The Overview started the Security Documentation strong. Great job on the Asset Inventory and Network Diagram. Only missing one service. Great job on the Hardening summary and business focused goals. Leadership will find this very useful. I especially liked that security is treated as on-going, not done once. The regular verification schedule highlights this.	which gives the impression it wasn't fully proofread before you sent it. • A few vulnerabilities, such as FTP and DNS settings, aren't clearly closed out or confirmed as fixed in the hardening section, so adding a follow-up note would make it more readable by an executive audience. • It would also help to add a short executive summary listing your most critical findings and fixes so that leadership can grasp the highlights quickly. • Finally, make sure every service or port listed in the asset inventory is also clearly explained in the vulnerability or mitigation sections, just to show how everything is tied together." • The vulnerability table, while comprehensive, lacks prioritization or analysis. It reads like a patch-management dump rather than a risk assessment. Next time, highlight which vulnerabilities were most critical or actively exploitable to show judgment. • I would have liked to see the System Overview more thoroughly describe the business concerns for Leadership. Impressive number of vulnerabilities identified! Would have liked to see more than CVE numbers and to apply a fix such as greater detail along with why this is done would have made the information more useful. HMI and PLC systems vulnerabilities should not have been mitigated, only identified. I really liked your Hardening Summary. The actual commands, KB/CVEs, and acronyms were not useful to Leadership. Missing list of tools and their costs. In the future recommend removing AI prompt.

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	858

Strong Points	Areas of Improvement
• Good job quantifying risks, such as the daily oil production loss and regulatory fines.	• Video was 7:43—far too long for an expected length of 5 minutes. Several slides

Strong Points	Areas of Improvement
• Your summary of the business and operational risks is clear, and the financial details are well-presented. Great work! • This teams' analysis of the incident and the risks are the best that I have seen! Samreen, Cedric, and Stephen are truly exemplars of explaining what happened and why this matters in clear financial terms that directly impact the bottom line. This isn't just the loss in revenue but specific details about various fines and estimates for equipment replacement—seriously, this was the most thoughtful approach I have seen in all the teams that I have seen and this alone would have made me sit up and pay attention, as you spoke to all of senior leadership in a way that truly mattered. Well done, team! • I loved Samreen's statements about ""technology protects systems but people protect companies"", that leadership accountability defense, and that services can be outsourced but not accountability. These are powerful statements. • The operational risk assessment clearly identifies how the risks affect the company's concerns and their bottom line and is appropriate for all C-suite executives. • The financial aspect was covered extensively. • Very thorough plan	in this were unnecessary such as the 'Leadership is the Firewall' slide. • Some slides were overloaded with words and details—it's best for slides to have minimal text and not overwhelm the listener with reading and listening at the same time. • Some technical jargon was used which, when used, should be defined/explained for all of the c-suite to understand. For instance, replay attacks, SOC monitoring, HMIs, and more are mentioned without explanation. • Beyond this, preventative measures and strategies as a whole weren't related to risks sufficiently, such as discussing future risks if recommendations aren't followed. • Areas for improvement is to ensure that you meet the time expectations, as the video exceeded 7 minutes. Additionally, consider reducing the technical jargon, given that the target audience is at the C-Suite level. The flow of the presentation was somewhat disjointed and could benefit from adjustments to better align with the rubric. • Let's set aside that this presentation clearly went long, and focus on the biggest problem here: The slides. First, it is pretty clear that this deck was put together like Frankenstein's monster, taking bit of one person and slapping these next to parts of another. There is only the vaguest cohesion in theme here. The first slides are overloaded with data. While all of this information is important (see above), is there a reason that all of these dense, text-heavy slides couldn't have all this incredible information spread out over two or more slides to make this easier to follow and digest? After these though, the slides start to get really spartan such as Lessons Learned and Preventative Measures, which are vague and general like "Third-party Supply Chain Weakness" and "Develop a Zero-trust Architecture," neither of which are telling us really what happened or how to prevent this from happening again. And then the style shifts again with the next slides, using tinier fonts and bolded text—but all this is so different from the end of the deck where suddenly there is just a title

Strong Points	*Areas of Improvement*
	and a large icon and on the penultimate slide that actually has the image of a pen (for some reason). I'm pretty sure that this is the only icon and photograph in the deck, and it just underscores that each person did their own part of this assignment without coordination or collaboration with the rest of the team. Next time you work on a group project, I want to challenge each of you to take responsibility not just for your portion but for the entire project. Presentations like this succeed or fail more with how cohesive and unified the team's messaging is rather than each of you trying to be your own stars and clearly not functioning as an organic unit. • The video was substantially longer than five minutes, the video introduction included the Team ID# on the title slide but was not referenced in the introductory speech, the introduction also did not explain the tie in to this scenario. The operational risk assessment for the scenario is the first point where this presentation ties into the project. The shotgun start to the video drastically reduced the professionalism, unfortunately. This team did provide a reasonable strategy to reduce risks that were relevant and previously identified. The team did recommend 1 or more high priority actions to improve the overall security posture of the system and provided complete and consistent reasoning for some of them. However there was no discussion of consequences if the actions were not taken and the actions proposed, like developing a zero trust architecture and a SOC require significant investment. • Practicing the timing for the presentation would avoid asking to go to the next slide. Reasoning for recommendations was not provided. • Refer to the assignment guidelines for time management, structure, and requirements.

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 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
0	0	0	0	0	0	0

Whack a Mole		
WAM1	WAM2	WAM3
125	125	0

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
510	2

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)
21	0	0	0	27	1	26	27	0	0	0

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
209.22	0.46%

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

Green Team Survey Comments
• Your site is down, we cannot connect to it! • The error message says 502 Bad Gateway • Site didn't load • 502 bad gateway error • 502 Bad Gateway • Site does not load • Could not reach http://Web.blue0053.cfc.local Good luck! • URL redirects to some sort of download. site doesn't even load • Site did not load. • Site doesn't load • Site did not load. • your site is down! • Can't reach the website. • Site did not load • site can't be reached • Sorry your site is still down • website didn't open • site cannot be reached • Site did not load • Tried a few times site continues to be down • 4:48 your site is down • 5:06 This site can’t be reached • website cannot be reached • site is unavailable • web.blue0053.cfc.local refused to connect.