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

GEORGIA INSTITUTE OF TECHNOLOGY

CYBER JACKETS

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 21 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	441	29.40%	45
Security Documentation	984	78.72%	62
C-Suite Panel	1095	87.60%	19
Red Team	2000	80.00%	4
Blue Team	1425	71.25%	79
Green Team Surveys	1075	71.67%	32
Deductions	0		
Overall	**7020**	**70.20%**	**32**

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	441

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

1	No
2	
3	
4	Yes
5	Yes
6	
7	
8	
9	No
10.1	Yes
10.2	Yes
10.3	Yes
10.4	Yes
10.5	Yes
10.6	Yes

10.7	Yes
10.8	Yes
10.9	Yes
11.1	Yes
11.2	Yes
11.3	Yes
11.4	Yes
11.5	Yes
11.6	
11.7	Yes
12	
13	No
14	
15	Yes
16	Yes

17	Yes
18	Yes
19	Yes
20	Yes
21	
22	
23	
24	
25	
26	
27.1	No
27.2	
28	
29	
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	984

Strong Points	*Areas of Improvement*
• Good ideas to use tools with Kali Linux and install an ELK stack • The team did a great job with their system hardening strategies, using specific, open-source tools for clear hardening objectives. • Fantastic job on describing a strategic approach to system hardening. Justification provided was thorough and it wasn't just a list of "we did this" and "we did that". Network diagram was good as well. • Plenty of vulnerabilities were enumerated. • All vulnerabilities are listed with specific fixes.	• System overview was not well defined. Not supposed to modify the assumed breach VMs • The system overview could use some more detail on what function each asset performs. Several key vulnerabilities were not identified. • Polish the system overview to clearly explain the purpose of every system to executive audience. Technical details are there already, but it needs a bit more of a big picture.

Strong Points	*Areas of Improvement*
• The document is organized and uses professional language.	• This did not feel like a cohesive document. Consider how best to present important information to senior leadership that may not have your level of expertise. • Lighter formatting and shorter tables would make reading easier. • More section headings and visual breaks improve clarity.

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	1095

Strong Points	*Areas of Improvement*
• Great high level intro/agenda. Great job including everyone and correlating everything together • Good explanation of risks • The presentation was presented professionally and cleaning with minimal distractions, reference to the Team ID number, and an appropriate dress code was followed. Acknowledgement was also given to all contributors. • The team provided a clear summary of the risks to the company with direct numerical impacts to the company's bottom lines and was presented in a manner that would be acceptable to all C-suite members. • The risk reduction strategy does provide a complete strategy to reduce risk both immediately and in the long term and clearly addresses the previously identified risks with a note to conducting an incident analysis to prevent future similar attacks. • Addresses forensic capture of devices • Well designed slides. • Good work on quantifying the risks. • Good work listing samples tools for immediate and long term actions. • Recommend to discuss staffing, software, and hardware requirements for the immediate actions. • Well researched. • Nice job highlighting EPA fines, as this is important for the industry and operational	• Longterm actions slide has too much content. Longterm tools is vaguely presented on why it is needed. • A better relation from risk-mitigation-recommendations. There are not clear short term and long term recommendations indicated and easy to follow. • The formatting on the slides was not consistent and negatively impacted the professional appearance. The presentation did meet the time requirement but included a section on similar attacks that didn't support the overall position of the presentation. The time that was spent on discussion other cyberattacks would have been better used to talk about how the proposed tools would be used to support the proposed high-priority actions. I would also recommend, for future projects, providing more clarity and differentiation between the strategy proposed to reduce risk and the high-priority recommendations. The team does propose high-priority action items that range from near to long term proposals. They are justified clearly with consistent reasoning however these actions do require additional funding. The section on Longterm [sic] Action Tooling meets other requirements of the project and are good recommendations but don't necessarily support the items detailed in the Longterm [sic] Actions slide.

Strong Points	*Areas of Improvement*
costs. Providing examples like Stuxnet, Colonial Pipeline and Triton give a solid explanation of the cause/effect	• How would two-person control have prevented this incident? • When switching between multiple presenters it is recommended for them to introduce themselves or introduce the next speaker. Another option would be to add the student name and role under the video. • Some jargon terms. Ensure phrasing is adequate for non IT experts. • For Long term actions would switch the focus on what the goal of the tools is and then discuss the related tools, rather than first focusing on the tools and then the uses. • Would recommend include a final references slides for those who would be interested in learning more about the similar cyber events and a list of all of the software mentioned for quick reference. • Connect the high priority recommendations to the initial attack and risks. Explain how the tools will be accessed

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
250	250	250	250	125	125	0

Whack a Mole		
WAM1	WAM2	WAM3
250	250	250

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
1425	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	23	26	27	23	27	27	24	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
1075

Green Team Survey Comments
• Footer not on home page • no footer on homepage • site is timing out. not loading properly • website not loading • Will not load website. • site does not load • homepage footer too high • The footer is not on every page. It is missing on the login page. Also, it is too high on the home page. • Nice job Team 21! • footer covers web elements • footer moves with scrollbar instead of staying at the bottom of the page • footer covers web elements

Green Team Survey Comments
• Rock-solid work! Even Obsidian Rift’s rigs approved though the login and signup pages are missing their footers. And that sticky footer? It’s making the page tough to read. Plus, your navbar logos seem to have swapped places :(• red user added, logos flipped around • Good work! All intended areas are still accounted for within the website and no issues locating anything per the requirements. Your ridge is currently not operational. • Site is down • "502 Bad Gateway nginx/1.19.0"