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

SLIPPERY ROCK UNIVERSITY

SLIP SECOPS

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 81 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	147	9.80%	90
Security Documentation	968	77.44%	65
C-Suite Panel	594	47.52%	91
Red Team	750	30.00%	53
Blue Team	860	43.00%	91
Green Team Surveys	11	0.73%	88
Deductions	0		
Overall	3330	33.30%	88

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	147

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

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

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

17	Yes
18	Yes
19	Yes
20	No
21	
22	
23	
24	
25	
26	
27.1	
27.2	
28	No
29	
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	968

Strong Points	*Areas of Improvement*
• The System Overview and the System Hardening recommendations are very well written and thoroughly described for the senior management audience. Additionally, the network diagram, although it is a picture of a diagram written on a whiteboard, shows all the logical connections to components on the network and includes a legend which is helpful for readability. • Network diagram was easy to read and understand. • The system hardening section is well written and thorough.	• There are some issues with format of the report and professional presentation. In the Asset Inventory list, this has some formatting issues and could be organized better. Instead of leaving unused lines in the table, it would be more readable to list the port and associated protocol as separate line items under the component. There are also large white spaces or possibly unused pages in the report. In the System Hardening section, which is again very well written and contains critical content, there are two section headers for

Strong Points	*Areas of Improvement*
- The system hardening section was excellent. - Your mitigation steps in the vulnerabilities section were well presented and showed real understanding of how to strengthen the system. Your system hardening work was also solid and demonstrated consistent effort across the assignment.	"System Hardening", so formatting could be improved to increase professional delivery of the information. - System overview didn't really talk about the purpose of the system in depth. No list of tools given. - Formatting should be consistent, at least in each section, if not through the whole report. Also I highly recommend learning to use a diagraming tool such as DrawIO which is free. - There were formatting issues, the vulnerabilities section is probably too technical for a c-suite audience. - This was a strong submission. Adding just a bit more detail in a few areas would help round everything out, but overall you should feel very confident in the quality of your work.

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	594

Strong Points	*Areas of Improvement*
- I can tell a lot of effort was put into creating this presentation. Good work on presenting as a ROI for the C Suite - Strong point for this entry was definitely risks to the core business and the financial impact this incident would have. Exposure slide was detailed with lots of relevant content that the C-Suite would likely be concerned about. Content of presentation shows technical aptitude and understanding. - Financial and Operational Risk Assessment: The team provided a clear summary of business and operational risks. They were highly effective in relating the specific cyber-physical attack (mirroring the TRITON/Trisis attack pattern) to the company's financial bottom line. This included citing a severe burn rate of 41.5 billion catastrophic loss avoided (referencing events like Deep Water Horizon and the BP oil spill cleanup). This demonstrated sophisticated insight into the	- Strongly recommend saving as a video an uploading, but am happy at least something was submitted. Videos were blocking large sections of content. Need more focus on the business and operational risks than just the incident itself. - Slides were very content-detailed and presentation went over allotted 5:00min with video content - additional slides without video content would likely add to that. Making the content more concise and cutting out irrelevant details may help. For example, C-Suite may not need all of the incident overview details as they would likely want more time spent to focus on the risks. Narrow the focus down away from technical details and only hit upon the big points that C-Suite may be concerned with. A broader overview of the strategic plan before jumping into individual recommendations may be a good way to center this presentation better.

Strong Points	*Areas of Improvement*
scale of risk and its effect on company concerns. • Comprehensive Strategy: The team delivered a complete strategy to reduce risk. This strategy included clear, long-term actions such as strengthening ICS network governance and segmentation, mandating strict separation between control/safety/business networks, enforcing MFA and least privilege access controls, and deploying zero trust network segmentation. This strategy was explicitly relevant and comprehensive in addressing the threat of persistent remote access and lateral movement. • ROI Justification: Although their recommendations ultimately required too much funding, the team provided strong complete and consistent reasoning and demonstrated an excellent understanding of Return on Investment (ROI). They effectively compared the proposed 5-year investment of $1.38M against the potential reactive costs of over $450M incurred during the incident response phase (Phase 1 + 2 and downtime) • solution was in the rights areas area technically • Excellent job! Your slides and visuals were very detailed and engaging. Great effort the presentation was informative and well put together	• Adherence to Funding Constraints (High Priority Recommendations): The team failed to meet the crucial requirement that high priority actions must require at most a minimal level of additional funding (e.g., use only free or open-source tools). The recommendations presented totaled 400K) and an OT Incident Response Retainer ($750K). To achieve a Proficient or Exemplary score in this category, the team must prioritize 3-4 actions that strictly leverage free or open-source tools (such as configuring an open-source firewall or installing an IDS/IPS), or cost-free policy updates (like recovery planning or policy updates). • Presentation Quality and Delivery: While the visual aids were professional, the presentation delivery could be improved. The team did not mention the roles of each team member, and although the verbal introduction acknowledged all four members, the slide only listed two presenters (""Nolan & Chryst""). Furthermore, one of the active presenters was observed to be reading and not focusing on the screen, which acts as a visual distraction and detracted from the overall professional appearance expected in a C-Suite briefing, The presentation was difficult to gauge the time as this was more on a PowerPoint presentation embedded with team pitch videos. • Team Member Roles: Although the team provided clear acknowledgment of all contributions in the introduction (meeting the Exemplary requirement for required elements), providing further context regarding the roles of each team member could have enhanced the professionalism and clarity of the presentation. • solution required investment & didn't lean on opensource at all. Separate slides with inlaid video was more work to get through. seemed rushed, and way too short, skipping over points on the Risk Mitigation plan altogether such as OT Incident response at $750 which would definitely want to be raised & justified and justified in this type of presentation.

Strong Points	*Areas of Improvement*
	- The video quality made it a bit difficult to hear at times. Your slides included great detail, but the verbal delivery could be clearer. Try becoming more comfortable with the material so you can present it more naturally like telling a story rather than reading directly from your notes. This comes with time of course :).

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	125	0	0	0	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
860	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)
0	0	27	3	27	3	27	27	4	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
11

Green Team Survey Comments
• Check your site general html stuff has been changed on you and status page is completely down! • Webpage did not load. Error message: 502 Bad Gateway • your site is down! • Site didn't load, got 502 bad gateway error • nginx error • Site unable to load • 502 Bad Gateway • 502 Error • site not reachable. • The page didn't open. The error message was '502 Bad Gateway.' • 502 Bad Gateway • Website would not load. Error message: 502 Bad Gateway • Website is down (502 bad gateway error) • "502 Bad Gateway nginx" • 502 Bad Gateway • your site is unreachable! • Site says bad gateway • Site says bad gateway • "502 Bad Gateway nginx" • "Hello Team 81 I kept receiving a 502 Bad Gateway error. • 502 bad gateway • 5:23 502 Bad Gateway • 502 Bad Gateway • 502 Bad Gateway