



IDAHO STATE UNIVERSITY

MAN IN THE BEAN

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 60 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	257	17.13%	82
Security Documentation	1114	89.12%	33
C-Suite Panel	882	70.56%	77
Red Team	1125	45.00%	35
Blue Team	1698	84.90%	50
Green Team Surveys	441	29.40%	68
Deductions	0		
Overall	5517	55.17%	68

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 | 257

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

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

10.7	
10.8	
10.9	
11.1	
11.2	
11.3	
11.4	
11.5	
11.6	
11.7	
12	
13	
14	
15	Yes
16	Yes

17	Yes
18	Yes
19	Yes
20	No
21	
22	
23	
24	No
25	
26	
27.1	No
27.2	
28	No
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 | 1114

Strong Points	Areas of Improvement
<ul style="list-style-type: none">The asset inventory is extensive and thorough, this also applies to the vulnerabilities and mitigations identified, the list seems to go above and beyond. The network diagram is excellent, easy to read, includes a legend, and shows all the connections, including the database connection. The investigation skills and details provided in the vulnerabilities and mitigations is evident. Finally the System Hardening provides a well-written narrative of recommendations to senior management.	<ul style="list-style-type: none">The content of this report is excellent, but it could be improved by a few simple things such as developing the System Overview further, it is very concise and really needs to provide more description of the components, mention the network design, and any possible areas of focus that might be more vulnerable. This will really grab and focus the attention of senior management. Additionally, there seems to be issues with formatting and header sections and then large white spaces. The header sections should be the title of that section, not the

Strong Points	Areas of Improvement
<ul style="list-style-type: none"> Network diagram is well done. Excellent job on vulnerabilities. Extensive asset enumeration Technically sound throughout and appropriate for audience 	<ul style="list-style-type: none"> instructions to the team, for example the section that should be Vulnerabilities and Mitigations, check that again. Finally, in the System Hardening section, it would be helpful to include the tools that used to implement each recommendation listed. More detail in the system overview. Give a complete overview of the system. What is it intended to do? Why does it exist? What are the components? Don't list unknown components in asset inventory or at least figure out what they are before listing them. The system hardening should not be a diary, but a list of steps, with justification, taken to harden each system. These should be written in a way that is repeatable in the future. When presenting vulnerabilities be sure to have mitigations or recommended mitigations Network diagram should have included additional components

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 | 882

Strong Points	Areas of Improvement
<ul style="list-style-type: none"> Strategy was good, highlighting good policy and procedure changes. Excellent coverage of "what if nothing is done". About the risk and solution Good work including the cost of no action. very business level wording for the opener & risks, also referencing deaths in a previous explosion will get attention. Very thorough high priority actions and breakdown. Introduction was very clear and professional. Overall detailed synopsis provided details regarding risk. Slide deck was clear and easy to follow. Provided controls and reasons for possible failure. Provided segmentation detail and prevention of loss of revenue. Device monitoring was a great mention. Charts and 	<ul style="list-style-type: none"> Biggest gap - risks were very lightly covered. Everything else should be building off of your identified risks. Strategies and high priority actions had no ties to the risks. slow down a bit to highlight the important topics of the presentation State the work done by the team members not presenting, how did they contribute. Nice use of phone on slide design. Risk = how much financial loss. More details on strategy and actions such as staff needs, training needs, hardware and software required. Timelines and costs should include an explanation of how they were calculated. Stating the company is in the business of making money is not a statement

Strong Points	Areas of Improvement
detailed data with timelines was a great add.	<p>appropriate for the C-Suite. For example, BP's mission statement is: "Our purpose is to deliver energy to the world, today and tomorrow"</p> <ul style="list-style-type: none"> • Could also include references list. • May wish to ask for questions via email. • more detail re Business Operations in the Risk section at the start. substantiate better how 2 weeks work of network segmentation isn't going to cost anything, without getting techy (e.g. reconfiguring equipment we've already got and have skills in house) - and \$1500 a unit for failsafe... how many units? And whilst the \$1Bn & 5 years for a new oil rig if catastrophic is big, it will also likely encounter "likelihood" questions; a major factor in risk balancing. • The risks are too general. They need to be explained, not just mentioned.

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	0	0	0	125	0	250

Whack a Mole		
WAM1	WAM2	WAM3
125	125	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
1310	388

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)
25	23	27	26	27	26	27	27	27	0	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
33949.02	75.44%

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
441

Green Team Survey Comments

- a lot of the site is down and incorrect! By this point please go down the full list!
- Site looks okay, but I had no access to the 'Admin Dashboard', there was no 'Login' button.
- Nothing worked. The links were dead. There was no login button just sign up. Careers link and oil rig status did not work. No logo or pictures.
- Missing login option. No oil rig picture. Slogan is incorrect. No jobs listed. Footer is incorrect. Status page does not work. No photos in header.
- "Internal Server Error InvalidArgumentException, Attribute [login] does not exist."
- Not properly formatted and errors.
- The site loads, and that's it.
- Internal Server Error
- a lot of missing items
- Site has some issues: company name wrong, missing logos, tag line is wrong, Status page as a DB error, footer is in correct, image missing on front counter, and login is not working
- I am met with a page that says Internal Server Error
- your background image and logos are missing, and your navigation bar isn't fully correct. you do not have an accurate footer, and none on the front page. your admins are gone, and so is your rig status page.

Green Team Survey Comments

- no image, status page is down, no footer on the homepage, the admin panel misses the user on the list
- Home page has been changed to something non related to assignment, company name wrong, status page gives SQL error
- Hello Team 60 a couple of steps were missing for your site. There is no a logo for the ObsidianRift and a logo for the Abyssal Pearl within the site navigation bar. Every time I click on the oil rig status I get this error: SQLSTATE[42S02]: Base table or view not found: 1146 Table 'laravel.production' doesn't exist (Connection: mysql_historian, SQL: select * from `production`). The main page is missing a footer text. When logging into the admin page the users 'blue@obsidianrift.oil' and 'green-admin@obsidianrift.oil' do not have the admin tags. There should be a photo banner with an Oil Rig on the home background image.
- not ObsidianRift Energy Co.
- no photo, status does not work, not 'ObsidianRift Energy Co.'
- website is down
- web.blue0053.cfc.local refused to connect.