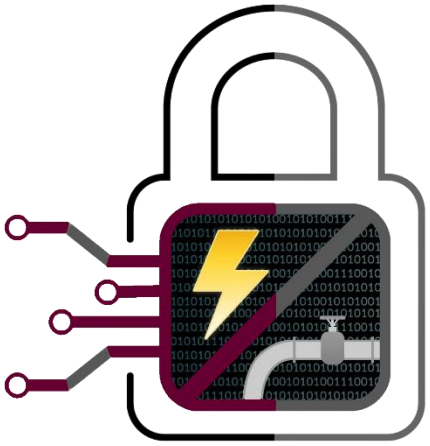


U.S. DEPARTMENT OF ENERGY'S

CYBERFORCE COMPETITION®

DEFENDING U.S. ENERGY INFRASTRUCTURE

C-SUITE INFORMATION

2025

CYBERFORCE COMPETITION®

CONTENTS

KEY DATES

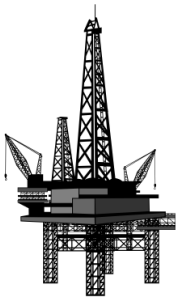
Monday, October 27, 2025	Students are provided with their C-Suite Scenario. Discord invitations are provided.
Tuesday, October 28, 2025 6:00pm CT (4:00pm PT)	C-Suite Fireside Chat *(optional & recorded)*
Monday, November 3, 2025 10:00am CT (8:00am PT)	C-Suite Panel video due
Monday, November 3, 2025	Students are provided with directions for accessing the rules. Students are provided with directions for accessing login information for their environment
Monday, November 3, 2025 6:00pm CT (4:00pm PT)	Rules Fireside Chat *(optional & recorded)*
Tuesday, November 4, 2025 6:00pm CT (4:00pm PT)	Security Documentation Fireside Chat *(optional & recorded)*
Friday, November 7, 2025 10:00am CT (8:00am PT)	*Late submission* deadline for C-Suite Panel video due
Monday, November 10, 2025 10:00am CT (8:00am PT)	Security Documentation due
Wednesday, November 12, 2025 10:00am CT (8:00am PT)	*Late submission* deadline for Security Documentation due
Friday, November 14, 2025 11:00am – 8:00pm CT @ Tinley Park Convention Center, Illinois	Students are provided with extended support hours with competition staff to answer any final questions. Red team and Blue team mandatory check in
Saturday, November 15, 2025	Competition Day

SCENARIO

FOR EDUCATIONAL PURPOSES ONLY – 2025 CYBERFORCE COMPETITION® SCENARIO

ObsidianRift Energy Co.

Abyssal Pearl



Incident Brief: ICS Compromise on Offshore Platform – Abyssal Pearl
Prepared for: ObsidianRift Energy Co. – Mobile Cybersecurity Response Team
Date: October 1, 2025
Location: Eastern Pacific Ocean, 200 nautical miles off the U.S. West Coast

---

Our newest and premier fixed offshore oil production platform, the Abyssal Pearl, has been in continuous operation for the past 18 months. The facility currently produces approximately 2,000 barrels of crude oil per day, supported by an integrated industrial control system (ICS) managing wellhead flow, separation, gas compression, flaring, and export operations. These barrels currently are the main source of crude oil for the Western areas of the United States.

An ongoing cyber event is affecting the Abyssal Pearl's ICS infrastructure. Preliminary findings suggest that the compromise originated from equipment introduced by a third-party maintenance contractor, who was onboard the platform for a brief period to service refrigeration units in the rig's galley.

Approximately eight days after the contractor's departure, platform personnel began observing intermittent communication disruptions within the ICS environment. This escalated into a complete 40-second blackout, resulting in all ICS devices simultaneously ceasing communication.

Two days ago, the situation escalated significantly, beginning with the gas compression system, which experienced an unexpected overpressure condition, resulting in a protective shutdown. All HMI terminals across the platform began displaying outdated system data, indicating a possible replay attack or historian compromise. Simultaneously, the flare pilot valve opened, but the igniter failed to activate, posing a severe risk of unburned gas release to the atmosphere. Although fire and gas detection systems remained operational, log data was discovered to be redirected to an unauthorized local storage node, suggesting deeper system manipulation.

As our corporate mobile cybersecurity response team, you are being deployed and stationed on-site at the Abyssal Pearl. Your primary mission is to conduct a comprehensive investigation into the suspected ICS compromise, contain any ongoing threat activity, and prevent escalation that could result in further production disruption, equipment damage, or risk to personnel safety. Your assessment and actions will be critical in determining the operational viability of the platform and guiding the next steps for recovery and system restoration.

FOR EDUCATIONAL PURPOSES ONLY – 2025 CYBERFORCE COMPETITION® SCENARIO

KEY RULES

The C-Suite Panel is a pre-recorded video based on the task described below. Record your video and upload it to a platform accessible to judges in the name format of TeamXXXX, indicating your team number (e.g., Google Drive, YouTube, Vimeo, Streamable). YOUTUBE LINKS ARE PREFERRED.

Before submitting, test your link to ensure it works. Then, submit the link in a text file (.txt) to the scoreboard by **MONDAY, NOVEMBER 3, 2025, AT 8AM PST**. Judges will begin reviewing videos shortly after.

- **Late submissions:** Accepted until **FRIDAY, NOVEMBER 7, 2025, AT 8AM PST**. Late submissions will receive a **25% score deduction**.
- **Accessibility requirement:** Your video must remain accessible from NOVEMBER 3–17, 2025.

C-SUITE PANEL

POINTS: 1250

The C-Suite Panel is a pre-recorded video based on the task provided below. This video should be recorded and placed somewhere accessible to judges. It can be Google Drive, YouTube, Vimeo, Streamable, etc. The preference is for you to submit a YouTube link. Please have other people test your link prior to submitting. Submit the link in a text file (.txt) for viewing to the scoreboard on or before **Monday, November 3, 2025, at 8 AM PST (10 AM CT)**. Judges will view your video shortly after. Late submissions will be accepted until **Friday, November 7, 2025, at 8 AM PST (10 AM CT)** to the scoreboard. Late submissions will lose 25% of the earned score. Your video must be accessible from Monday, November 3 – Monday, November 17, 2025.

TASK:

As the mobile cybersecurity response team for ObsidianRift Energy Co, you are being deployed to the Abyssal Pearl platform. The current status of the platform's ICS infrastructure is unstable. You've been tasked to investigate the suspected ICS compromise, contain any ongoing threat activity, and prevent escalation that could lead to additional impacts. ObsidianRift Energy depends on this platform, and is **concerned with production disruption, equipment damage, and personnel safety.** In addition, the C-Suite is concerned about long-term risks to the company's reputation and business.

The C-Suite wants a briefing next Monday (11/3/2025) about the operational and business risks posed to ObsidianRift Energy Co. You know that an understanding of the platform's network architecture is a key factor in your risk determination. Unfortunately, the network investigation team is still in the process of mapping the Abyssal Pearl's network(s) and its assets. They won't be able to provide any detailed data until next week. However, the team is confident that the disruptions are contained to the Abyssal Pearl platform and its ICS components, and not the larger enterprise IT network. Therefore, you will focus your C-Suite briefing on identifying and reducing risks associated with ObsidianRift Energy Co's operational and business concerns, rather than a technical walk-through of vulnerable network assets.

Your team has been asked to submit a recorded five (5) minute presentation to the C-Suite discussing:

- The risks posed by ongoing or further threat activity on the Abyssal Pearl network(s) that are directly related to ObsidianRift Energy Co's concerns (product disruption, equipment damage, safety, overall business for example).
- A summary of your strategy to contain and reduce the current risks you have identified, as well as prevent a similar attack against Obsidian Rift's other platforms in the future.

- High priority recommendations to protect the Abyssal Pearl's network infrastructure and ICS while sustaining business continuity throughout the process. Be sure to address mitigation of future risks directly related to concerns you have already noted.

The cyber event scenario details are available at https://cyberforce.energy.gov/cyberforce-competition/scenario/ and listed on page 3. A rubric table is provided that clearly shows scoring associated with required items.

Your video presentation should include the following:

1. Your five (5) minute video must start with your Team ID #. You may also include your first names or a team name but do NOT include any university identifiers. Participation of at least two members in the recorded video is expected, and contributions of other team members should be specifically acknowledged in your video.
2. Brief the C-Suite regarding the operational and business risks posed to the company by recent/ongoing, and future cybersecurity events.
3. Provide a summary of your strategy to reduce the identified risks as part of your response to the ongoing threat activity. Although the company does not specify financial risks, their concerns are tied to their bottom line.
4. Provide 3-4* high priority actions you will implement to improve the overall security posture of the ICS and larger network system or specifically address future concerns related to product disruption, equipment damage, safety, and business in general. Keep in mind that the C-Suite is primarily non-technical audience, and that current funding is extremely limited (or non-existent) and all actions you are taking should use free or open-source tools (for the business).
    a. Include and discuss any recommended staff communication, training, potential staff/management/policy changes that could help remediate the effects of the incident, reduce risk of future attacks, and improve the company's security posture. Highlight any future assessment and monitoring actions you propose.
    b. Discuss any additional resources (tools, staffing, capabilities, etc.) that are needed to implement your recommendations.
    c. Include a high-level summary of the estimated cost, timeline, and benefits/ justifications for your proposed recommendations.
    d. Briefly discuss the risks of similar cyber events occurring in the future if the company doesn't follow your recommendations. Although you don't yet have a comprehensive understanding of the company's network infrastructure, this discussion should be a persuasive pitch as to why your recommendations are essential for overall security and continuity of operations.

* Note: There are dozens of recommendations that you could make, but the C-Suite is extremely busy so you will need to prioritize your top three or four recommendations to present to the C-Suite in "tomorrow's" briefing.

C-SUITE PANEL BRIEF (VIDEO) RUBRIC

C-Suite Panel Rubric	Not Present 0	Emerging 1	Developing 2	Proficient 3	Exemplary 4
Presentation Time, Required Elements (2%)	• Required elements are missing. • Video file has no sound, is corrupt, or unviewable by the scoring team.	• Video introduction does not include Team ID# • Video is significantly shorter or longer than 5 minutes. • Only one team member can be identified as a participant in any way.	• Video includes Team ID#. • Video is longer or shorter than ~5 minutes (less than 3 minutes or more than 7 minutes). • Only one team member is an active presenter. • Additional team members are acknowledged.	• Video includes Team ID#. • Video length is approximately 5 minutes but too long or too short for amount of relevant information provided. • Two equally active presenters are in the video. • Acknowledgement of contributions from some team members.	• Video includes Team ID#. • Video length is approximately 5 minutes, and all the time is used well. • Two or more active team members participate equally. • Clear acknowledgment of contributions from all (either on- or off-screen) team members.
Risks *Related to Operational and Business Concerns* (30%)	• Content does not address risks or risks are not related to the scenario.	• Risks not related to business or operational concerns.	• Minimal summary of risks. • Minimal discussion of risks related to the company or its operational concerns and bottom line (finances).	• Summarizes business risks with some emphasis on how they affect the financial bottom line. • Risks are addressed in isolation (e.g., data, network control, uptime, and safety are analyzed separately). • Presentation is suitable for only some members of the C-Suite (e.g., excessive jargon and technical details that only the CIO and CTO can follow).	• Clear summary of business and operational risks. • Clearly identifies how risks affect the company's concerns and their bottom line (finances). • Presentation is suitable for all members of the C-Suite (e.g., jargon is avoided).
Strategy to Reduce Risks (30%)	• Content does not address business and operational risk reduction	• Provides no strategy or strategic plan of action for risk reduction.	• Provides a minimal strategy to reduce risks (e.g., only one action item or policy update). • Strategy does not directly relate to the previously identified risks.	• Provides a reasonable strategy to reduce risks (e.g., at least two long-term action items and/or policy updates). • Strategy relates to the previously identified risks.	• Provides a complete strategy to reduce risk (e.g., three or more long-term action items and/or policy updates). • Strategy clearly addresses the previously identified risks.
High Priority Recommendations (30%)	• Content does not provide recommendations of any kind.	• Recommendations are not high priority or are inappropriate for leadership action. • Missing justifications for proposed actions. • Recommendations do not relate to the provided scenario.	• Recommended 1 or more high priority actions to improve the overall security posture of the system. • Complete and consistent reasoning is provided for at least one action. • No discussion of future risks if recommendations are not followed. • Actions require significant additional funding (e.g., use of commercial tools).	• Recommended 2 or more high priority actions to improve the overall security posture of the system. • Complete and consistent reasoning is provided for at least two actions. • No reasoning is provided for why recommendations would reduce identified risks. • Actions require additional funding (e.g., mixed use of commercial, free, and open-source tools).	• Recommended 3-4 high priority actions to improve overall security and protect business continuity. • Complete and consistent reasoning for all actions is provided. • Reasoning is provided for why recommendations would reduce identified risks. • Actions require at most a minimal level of additional funding (e.g., use only free or open-source tools).
Quality of Presentation (8%)	• Presentation does not follow scenario guidelines.	• Inappropriate dress code—team is not dressed for a work environment. • Many visual distractions. • Inappropriate visual aids, slides or other on-screen materials.	• Appropriate dress code—team is dressed for a work environment. • Minor visual distractions. • Visual aids, slides or other materials lack professionalism.	• Appropriate dress code—team is dressed for a work environment. • Few visual distractions. • Visual aids, slides and other materials are acceptable.	• Appropriate dress code—team is dressed for a work environment. • Visual aids, slides and other materials have a consistent, professional appearance.