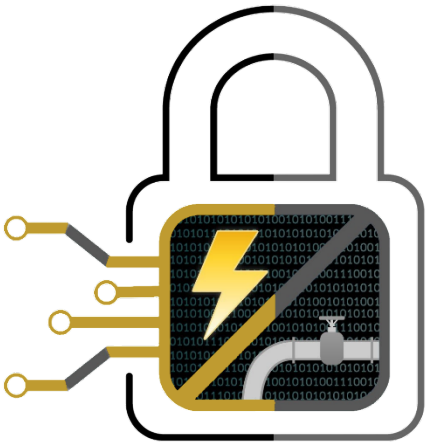

U.S. DEPARTMENT OF ENERGY'S

CYBERFORCE COMPETITION®

DEFENDING U.S. ENERGY INFRASTRUCTURE

C-SUITE INFORMATION

2024

CYBERFORCE COMPETITION®

CONTENTS

COMPETITION OVERVIEW

OVERVIEW

The CyberForce Competition® has been a pinnacle of workforce development for the Department of Energy (DOE), national laboratories, and industry. Through the CyberForce Competition, DOE has worked to increase 1) hands-on cyber education to college students and professionals, 2) awareness into the critical infrastructure and cyber security nexus, and 3) basic understanding of cyber security within a real-world scenario.

NOTE TO PARTICIPANTS

- For the purposes of competition, you are the **BLUE TEAM**.
- Overall scoring breakdown can be found later in this document. **PLEASE TAKE A MOMENT TO REVIEW THIS DOCUMENT THOROUGHLY**.
- This year, each team will be provided six (6) ethernet cables to connect to the internet. It is each participant's responsibility to bring the appropriate dongle or connector for their machine as nothing will be provided. Wireless connection will still be available.

KEY DATES

Monday, October 21, 2024	Students are provided directions for accessing the rules. Discord invitation is provided.
Tuesday, October 22, 2024 4:00 PT	C-Suite Fireside Chat *(optional & recorded)*
Thursday, October 24, 2024 4:00pm PT	Rules Fireside Chat *(optional & recorded)*
Monday, October 28, 2024 8:00am PT	C-Suite Panel video due
Monday, October 28, 2024	Students are provided directions for accessing login information for their environment
Tuesday, October 29, 2024 4:00pm PT	Security Documentation Fireside Chat *(optional & recorded)*
Friday, November 1, 2024 8:00am PT	*Late submission* deadline for C-Suite Panel video due
Monday, November 4, 2024 8:00am PT	Security Documentation due
Wednesday, November 6, 2024 8:00am PT	*Late submission* deadline for Security Documentation due
Friday, November 8, 2024 11:00am – 8:00pm CT @ Q Center, Illinois	Students are provided with extended help support hours with competition staff to answer any final questions. Red team and Blue team mandatory check in
Saturday, November 9, 2024	Competition Day

FOR EDUCATIONAL PURPOSES ONLY
2024 CYBERFORCE COMPETITION® SCENARIO

INTELLIGENCE BULLETIN

help@cyberforceisac.com | Phone: 202-555-2525 | Fax: 202-555-2626

CFC-2024-02

Cascading Consequences Seen after Energy Company Cyber Attack

Executive Summary

Between February 2024 and June 2024, a wind energy company within our area of responsibility (AOR) has identified a significant cyber breach to both its internal business network and operational network. This was previously reported in our CFC-2024-01 Intelligence Bulletin. This bulletin is to highlight the new information received from stakeholders.

While vulnerability mitigation efforts are underway, the wind energy company continues to see degraded energy output to those within their service area. Outages have been reported.

The threat is still imminent until the wind energy cyber team has been able to remedy all their systems which is not planned until mid-October.

The CyberForce Information Sharing and Analysis Center (ISAC) assesses with **HIGH** confidence the following points:

- The AOR has many key government facilities which are likely to be impacted.
- The AOR has the largest government-run AI-driven data center operating on clean energy, which is likely to be impacted.

Recommendations

The CyberForce ISAC recommends the following:

- Identify key dependencies within your AOR that may become critical if energy is lost or degraded.
- Identify potential resources and data sets that may be impacted and identify potential alternative options.
- Identify and remediate all known vulnerabilities within the system to ensure stable infrastructure.
- Ensure inventories include not only your dependencies but those that are dependent upon you.

FOR EDUCATIONAL PURPOSES ONLY
2024 CYBERFORCE COMPETITION® SCENARIO

KEY RULES

- **C-Suite Panel submission video is due no later than 8:00AM PT on Monday, October 28, 2024**. Teams will submit the link to their C-Suite Panel video in a text file (.txt) to the scoreboard. Late submissions will be accepted until Friday, November 1, 2024 at 8AM PT to the Scoreboard. *Late submissions will lose 25% of the earned score*. Please refer to the Scoring Breakdown for more information. Please ensure your video follows the format: <TEAM NUMBER_CSUITE>.TXT (e.g., 0000_CSUITE.TXT, 0987_CSUITE.TXT).

ORANGE TEAM SCORING

TOTAL POINTS: 2000

C-SUITE PANEL BRIEF

POINTS: 1000

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, October 28, 2024, at 8AM PT**. Judges will view your video beginning October 28. Late submissions will be accepted until Friday, November 1, 2024, at 8AM PT to the scoreboard. *Late submissions will lose 25% of the earned score.* Your video must be accessible from Monday, October 28 – Monday, November 11, 2024.

TASK:

Energia Ventosa's core mission involves supplying reliable, clean energy to its area of responsibility (AOR). Within that AOR are key government facilities and the largest government-run AI-driven data center operating on clean energy. The C-Suite (CEO, CIO, and COO) is concerned that the continual energy output degradation resulting from the cyber breach may impact the Energia Ventosa's business. What are the risks to the Energia Ventosa's core mission of supplying its AOR with reliable, clean energy if systems continue to be compromised and degraded within the service area?

The C-Suite wants a briefing next Monday (October 28, 2024) about the risks posed to the company by the ongoing effects of the cyber breach. You know that an understanding of the company's business and operational network architectures is a key factor in your risk determination. Unfortunately, the network admin team is still in the process of mapping your network and its assets. (Note: you assigned this task to them a month ago, but the network admin team is severely understaffed and behind schedule.) They won't be able to provide you with any data until next week. In the meantime, they assured you that there are security measures in place which mitigate further external threats and isolate the effects of the breach. Therefore, you have decided to focus the corporate briefing on the business risks of the cyber breach, rather than a technical walk-thru of vulnerable network assets.

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

- The risks to the Energia Ventosa's core business if facilities in the AOR continue to experience degraded energy output and outages.
- A summary of your strategy to reduce identified risks to the AOR.

- High priority recommendations to protect your network infrastructures while sustaining business continuity throughout the process.
- Risks of similar events happening in the future if the company doesn't adhere to your recommendations.

The 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 acknowledged.*
2. Brief the C-Suite regarding the risks posed to the company and its bottom line (i.e., focus on the business risks) by the continual degraded energy output and outages experienced by government facilities in the AOR.
3. Provide a summary of your strategy to reduce the previously identified business risks as part of your response to the breach.
4. Provide 3-4* high priority actions you will implement to improve the overall security posture of the system. Keep in mind that the C-Suite is a 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 changes that could help remediate the effects of the breach, reduce risk of future attacks, and improve the Energia Ventosa'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.

** 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.*

5. Briefly discuss the risks of similar 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 should be a persuasive pitch as to why your recommendations are essential.

RUBRICS

C-SUITE PANEL BRIEF (VIDEO) RUBRIC

C-Suite Panel Rubric	Not Provided 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, contributions of other team members are minimal.	• 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 (but other team members' contributions are not noted).	• Video includes Team ID#. • Video length is approximately 5 minutes, and all of the time is used well. • Two or more team members participate equally. • There is clear acknowledgment of contributions made by any off-screen team members.
Risks to Core Business (30%)	• Content does not address risk or risks are not related to the scenario.	• Risks not related to business concerns.	• Minimal summary of risks. • Minimal discussion of risks related to core business.	• Summarizes core business risk via relationship to degraded energy output. • Business risks and are addressed in isolation (e.g., minimal discussion of how the breach and future breaches will impact the core business). • 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).	• Summarizes both core business and customer's risk. • Clearly identifies how the breach and degraded energy output will affect core business. • Presentation is suitable for all members of the C-Suite (e.g., jargon is avoided).
Strategy to Reduce Risks (30%)	• Content does not address 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 identified core business 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 identified core business 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 identified core business 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 protect infrastructure. • Incomplete or inconsistent reasoning for all proposed actions • Actions require significant additional funding (e.g., use of commercial tools).	• Recommended 2 or more high priority actions to protect infrastructure. • Complete and consistent reasoning is provided for at least one action. • Actions require additional funding (mostly free or open-source tools).	• Recommended 3-4 high priority actions to protect business continuity through increased overall security posture. • Complete and consistent reasoning for all actions is provided. • Actions require at most a minimal level of additional funding (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.