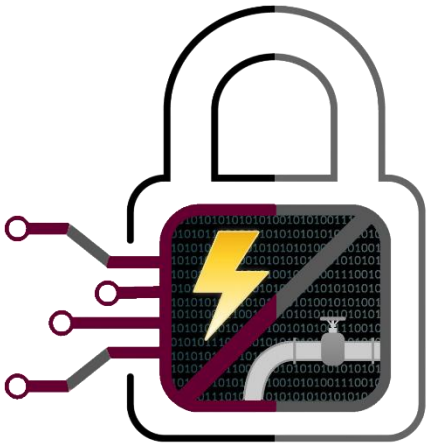


U.S. DEPARTMENT OF ENERGY'S

CYBERFORCE COMPETITION®

DEFENDING U.S. ENERGY INFRASTRUCTURE

OVERVIEW, RULES, & SCORING

2025

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 since 2016. Through the CyberForce Competition, DOE has worked to increase 1) hands-on cyber education to college students and professionals, 2) awareness of 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 AND COMPLETELY**.
- 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 connections will still be available.

KEY DATES

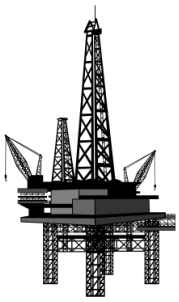
Monday, October 27, 2025	Students are provided with their C-Suite Scenario. Students are provided with instructions to log into the controller.
Tuesday, October 28, 2025 6:00pm CT (4:00pm PT)	C-Suite Fireside Chat *(optional & recorded)*
Monday, November 3, 2025 10:00am CT (8:00am PT)	C-Suite Panel video due
Monday, November 3, 2025	Students are provided with directions for accessing the rules. Students are provided with access to AWS.
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 help 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

COMPETITION STRUCTURE

COMMUNICATION FLOW

For the remainder of this document, students are classified as the **BLUE TEAM**.

Blue	A Blue team is composed of collegiate students who defend their network infrastructure from the Red team and maintain system usability for the Green team.
Red	The Red team includes industry security professionals that play the role of cyber attackers or "hackers" attempting to breach the Blue network infrastructure and defenses of the Blue team participants.
Green	The Green team includes volunteers with a variety of skill sets, to emulate typical end users.
White	The White team includes national laboratory employees who support the participants in setting up their infrastructure and judge the competition.
Orange	The Orange team includes volunteers who play the role of a C-suite within a mock organization who review videos and security documentation.

SETUP PHASE

Blue teams will be given access to their AWS environment no later than Monday, November 3, 2025. Blue teams should use this time to assess, build, secure, and test their system prior to the competition as well as familiarizing themselves with the competition scenario. Blue teams should continue to prepare their Security Documentation and their C-Suite video until their due dates.

ATTACK PHASE

On the day of the competition (Saturday, November 15), the Red team will attempt to gain access to Blue team services on the traditional infrastructure and already have access to the assume breach infrastructure. Meanwhile, the Green team will be responsible for evaluating the Blue team's web services and system operations. The White team will assess Blue team service uptime. Throughout the competition, Blue teams must monitor their systems, answer anomalies, and maintain their website for Green team users.

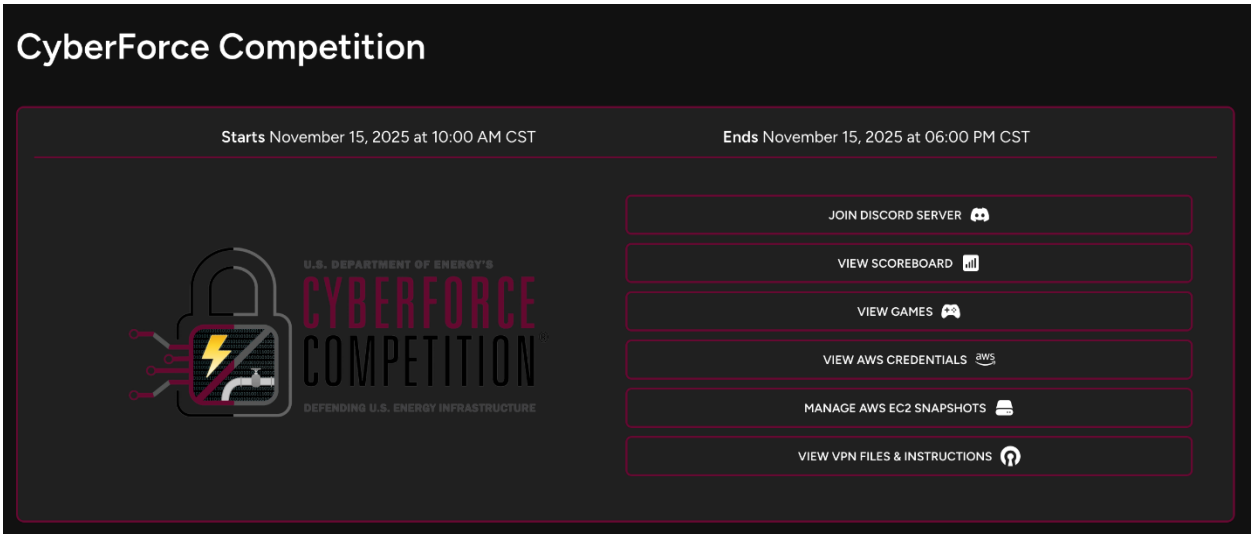
During this phase, Blue teams may not receive help from anyone external from the 4-6 members on a team. Receiving help from others, including mentors, external parties, etc., will result in disqualification.

GETTING STARTED: PRE-COMPETITION

CONTROLLER

Students and mentors will need to visit HTTPS://CONTROLLER.CYBERFORCECOMPETITION.COM/ and register using the .edu email you registered with for the competition (the one you have been receiving emails to). *If you participated in the 2024 CyberForce Competition or either of the 2025 Conquer the Hill Command or Reign competitions AND you used the same email to register; you will already have an account.* There is a "Forgot password" function available.

This will be the main dashboard that will be used for navigating your competition needs. It will be where you join Discord, view the Scoreboard, participate in CyberForce games for raffle tickets, get your AWS Credentials, manage your AWS snapshots, and get your VPN files. *Note*: not all items will be available right away.



DISCORD

- Discord is **required** for support throughout the competition timeframe. There will not be any technical support for students via email leading up to the competition or in-person on the day of.

NAMING CONVENTION

- By joining the competition Discord server via the controller, students and mentors will auto-populate with their team number as a prefix to their name. This will add each student to their team's red-blue bridge channel and provide them with the Blue Team role/access. Mentors will **NOT** be added to the bridge channel but will be provided with the Mentor role/access.
- In the event you need your nickname changed (e.g., you don't go by your full name), please submit a "Controller" ticket type and provide the name you do use. This must be appropriate, and staff have the right to not accept a request.

DISCORD RULES & SUPPORT

- Tampering with Discord bots, channels, or other teams' tickets will result in disqualification.
- Participants are encouraged to assist one another in the designated Discord channels, except for providing answers for anomalies or other scored items during the competition.
- **DO NOT DM** admins or staff, each violation will result in a 10-point deduction.

HELP DESK

If students need technical help from the White Team, they must submit a help desk ticket **in Discord**. The help desk is monitored only during regular business hours (Monday–Friday, 8am-5pm CT) before the competition. Tickets will be monitored all day Friday, November 14 and Saturday, November 15 with shorter response rate requirements. It is the responsibility of the **ticket submitter** to ensure they are responding to questions/answers promptly

- The Help Desk will operate via the #ticket-system channel.
    - Students needing assistance before or during the competition must submit a ticket.
    - Additional ticket types may be announced as needed.
    - Please only submit one ticket per issue and be cognizant of which ticket type you select.

- When submitting a ticket, be as specific as possible and select the correct topic. Avoid combining unrelated issues into one ticket.
- Check the *#announcements* and *#documentation* channels for updates **before** creating a ticket.

EMAIL

Students may email CyberForceCompetition@anl.gov for LOGISTICAL ISSUES ONLY. Please note, this email is only monitored during normal business hours (Monday–Friday, 8am-5pm CT). This email will not be monitored Thursday, November 13 – Saturday, November 15, 2025, please be sure to use the help desk system.

COMPETITION ENVIRONMENT

NETWORK TOPOLOGY

- You will inherit a /27 AWS VPC subnet
- Any changes to your Blue team infrastructure must be clearly documented in Security Documentation.

LOGIN INSTRUCTIONS

VPN INSTALL INSTRUCTIONS

The competition uses OpenVPN for access to the AWS environment. You will be provided with an OVPN configuration file to connect to your network. Students should be mindful that we support only these community clients for each operating system can be found below:

- Windows – OpenVPN Community - https://openvpn.net/community-downloads/
  - Place the OVPN file into "C:\Program Files\Openvpn\config".
- MacOS – Tunnelblick - https://www.tunnelblick.net or https://openvpn.net/client-connect-vpn-for-mac-os/
  - Double click the OVPN file to import it to Tunnelblick
- Linux – sudo apt (or yum) install openvpn
  - Run "openvpn --config YOUR_OVPN_FILE.ovpn"

AWS & SCOREBOARD CREDENTIALS

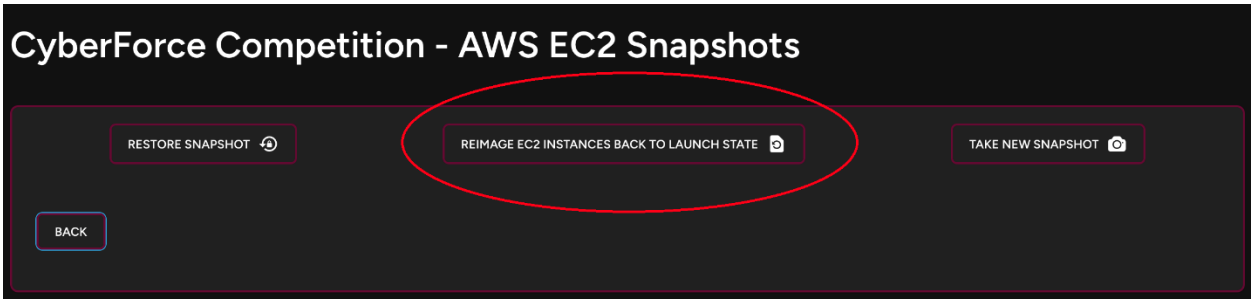
Students will need to visit HTTPS://CONTROLLER.CYBERFORCECOMPETITION.COM/ site as mentioned above to receive their AWS credentials or utilize the scoreboard. It is each team member's responsibility to ensure they register with the controller to ensure they get adequate time to prepare. Within the controller, you can sign into AWS, reset your AWS password, and download your team's VPN files. Additional instructions are available in the CyberForce Competition AWS document.

- Limits have been placed on *snapshot revert* to 2 reverts per VM per hour.
- IAM password reset cooldown every 15 minutes.

Scored services can be tested the week before the competition. Services should be connected by Friday, November 14, 2025, to ensure that scoring is accurate as soon as the competition starts. It is each team's responsibility to input C-Suite submissions, Security Documentation submissions, etc. into the scoreboard.

RESTORING SYSTEMS TO INITIAL STATE

If a Blue team damages any virtual machines beyond the point of recovery, you may restore to a fresh, default image of the system using the Controller. However, your team will incur a scoring penalty of **150 points per VM restoration**. To prevent a scoring penalty, your team is encouraged to create disk snapshots of each system as it is set up and configured, especially before and after any significant infrastructure changes.



KEY RULES

- **No Offensive Actions**: Blue team participants may not engage in offensive actions against other Blue teams, the Red team, the Green team, scoreboard, the competition network/infrastructure, or the hosting venue infrastructure/network. Violations will result in disqualification.
- **Team Number Usage**: Use the provided Excel document to find your specific four-digit team number whenever "BLUEXXXX" or "TEAMNUMBER" is referenced.
- **AWS Access**: Blue team members will have AWS environment access by November 3, 2025. Administrative accounts are managed by the White team and will only be used for scoring and rule enforcement.
- **Confidentiality**: Communications with the White team are confidential.
- **Rule Updates**: Updated rules are available on the CyberForce Competition GitHub and the Discord #announcements and #documentation channels. Participants are responsible for being informed of updates.

ALLOWED ACTIONS

- **Secure existing required services** on provided traditional VMs on their standard ports throughout the entire competition.
- **Harden/modify** any aspect of the following Traditional Infrastructure designated VMs (unless otherwise called out in the documentation): Database (Windows 2022), Active Directory (Windows 2019), Task (Ubuntu 22), and the Webserver (OpenSUSE Leap).
- **Move and configure non-required services** within the traditional infrastructure.
- Use **only free or open-source software**; free trial software is ok if a credit card is not required and support from staff is not required. Additional AWS security software that is not inherent within your system is not allowed.
- Create **EC2 VM snapshots**.
- **Deploy innovative defense strategies** within rule constraints.
- Sign up for a **mandatory** Red-Blue check-in on Discord for November 14, 2025.
    - https://calendly.com/cyberforcecompetition/2025-cyberforce-red-blue-check-in
- **Help desk tickets** are required for support before and during the competition. No assistance in-person other than networking issues will be provided.

- Tickets are **NOT** to verify answers or provide step-by-step actions for your infrastructure. Please ensure you have reviewed the rules, guidelines, and all material thoroughly and have done research prior to submitting a ticket.

PROHIBITED ACTIONS

- **No additional VMs**: The environment is limited to **SIX** VMs.
- **No deleting provided machines**: If needed, restore from a snapshot instead.
- **No modification of the following users**: SCORE1 & SCORE2 on traditional infrastructure.
- **Use extreme caution before modifying any Assume Breach VMs** (PLC: Ubuntu 22 & HMI: Windows Server 2019). Any change that disrupts scoring or Red Team engagement can cost your team Red points. While monitoring tools may be installed, teams do so at their own risk, modifications that impact VM resources or usability may cost your team points.
- **No blocking ports** on Assume Breach VMs or Traditional VMs.
- **No branding** website, documentation, or video with university information.
- **No IP or machine name changes** to provided VMs.
- **No offensive actions** toward other Blue teams, the Red team, the Green team, scoreboard, the competition network/infrastructure, or the hosting venue infrastructure/network.
- **No AI tools** (e.g., ChatGPT) for anomaly resolution or infrastructure defense.

COMPETITION REQUIREMENTS

REQUIRED SERVICES AND PORT NUMBERS

All Blue teams are required to maintain the following services on the listed ports during the competition. If one of these services is on a provided VM, it must remain on that VM. If it is not there, it is the Blue team's responsibility to create that service on that port within that VM. This pre-existing service will be scored.

SERVICE	PORT #	BOX
HTTP	80	OpenSUSE Leap
IMAP	993/143	TASK Ubuntu 22
WinRM	5985/5986	Win19
phpmyadmin	80	Win22

SERVICE	PORT #	BOX
NFS	111/2049	OpenSUSE Leap
SNMP	161	Win22
SMB	139/445	TASK Ubuntu 22
MariaDB	3306	Win22

SERVICE	PORT #	BOX
LDAP	389	Win19
SSH	22	TASK Ubuntu 22
SMTP	25	TASK Ubuntu 22

SCORING BREAKDOWN

Red Team	2500 points	25%
Blue Team	2000 points	20%
Green Team	1500 points	15%
Orange Team	2500 points	25%
Anomaly Scoring	1500 points	15%
Total	**10000 points**	**100%**

RED TEAM SCORING

TOTAL POINTS: 2500

- **Assume Breach** (1000 points): Teams must investigate and report attacks on Assume Breach VMs.
- **External Pentesting** (1500 points): Automated scans and penetration testing sessions.
- **Friday Red-Blue Check-in MANDATORY**:
  - Teams must check in with a Red team member on **November 14, 2025.** Check-ins begin at 11am and are 15 min in length and the final time slot is at 7:45pm CT.
  - Schedule your time: https://calendly.com/cyberforcecompetition/2025-cyberforce-red-blue-check-in

BLUE TEAM SCORING

TOTAL POINTS: 2000

- Service uptime and Oil Rig production progress.
- Points awarded for successfully maintaining the required operational services (p. 8) on their mandatory ports.

GREEN TEAM SCORING

TOTAL POINTS: 1500

TEAMS MUST UTILIZE THE WEBSITE PROVIDED FOR THEIR GREEN TEAM SCORING.

- Teams should review the Green team survey rubric and ensure their website meets outlined requirements.
- Your team must, the best of their ability, complete the website so that each of the questions below would be answered in the "True" statement.
- Green users are provided the "golden copy" images to validate your website against.
- Utilize only the images provided by the competition staff and **do not rename the images**.
- The website that Green team will be testing must be found on the Webserver VM.

ORANGE TEAM SCORING

TOTAL POINTS: 2500

C-SUITE PANEL BRIEF

POINTS: 1250

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 (e.g., Google Drive, YouTube, Vimeo, Streamable). YOUTUBE LINKS ARE PREFERRED. The 2025 Scenario can be found in Github.

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.

SECURITY DOCUMENTATION

POINTS: 1250

Blue team participants should use the Security Documentation to showcase their unique approaches to securing their infrastructure.

SUBMISSION REQUIREMENTS

- Use the **2025 CyberForce Competition Security Documentation Template**.
- Do **not** include university names, personal details, or any other identifying information, only your team number.
- Refer to the **2025 SecDoc Network Diagram Examples** for guidance.
- Submit your documentation as a **PDF** on the scoreboard by **MONDAY, NOVEMBER 10, 2025, AT 8AM PT**.
- **Late submissions** will be accepted until **WEDNESDAY, NOVEMBER 12, 2025, AT 8AM PT**, with a **25% score deduction**.

CONTENT EXPECTATIONS

- Documentation should cover **all infrastructure**, including **Assume Breach VMs***.
- Your role is to:
  - **Identify vulnerabilities** in the Assume Breach VMs.
  - **Identify and remediate vulnerabilities** in the Traditional VMs.
- Remember, this competition simulates a real-world scenario. **Presentation and professionalism** will influence your final score.

*** REMEMBER TO REFER TO THE ALLOWED AND PROHIBITED ACTIONS SECTIONS IN REGARD TO WHAT IS ALLOWED IN THE ASSUME BREACH VMS.**

ANOMALY SCORING

TOTAL POINTS: 1500

- Provided via USB on Friday, November 14.
- Password-protected files: attempting early access results in penalties.
  - Windows users will need 7zip or WinRAR to unzip the folder.
  - Linux and Unix users will utilize the gpg command.
- **Scoreboard Rules:**
  - Multiple attempts allowed for some anomalies.
  - Proper syntax required (case sensitivity indicated in question hints).

SUGGESTED SOFTWARE

Below is a list of software that is not required but will be extremely helpful in solving anomalies.

TOOL	PURPOSE
Steghide	Steganography decoding
John the Ripper, hashcat	Password cracking tool
NMAP	Network mapping
Outlook or VSCode to preview EML	Needed for an anomaly
CyberChef	Needed for an anomaly
Python	Needed for an anomaly

Universal Radio Hacker (URH)	Needed for an anomaly
Docker	Needed for an anomaly
Git	Needed for an anomaly
Autopsy	Needed for an anomaly
GCC-12	Sudo apt install or from tarball
Clang-14	Sudo apt install or from tarball
Make	Needed for an anomaly
WinDebug	Needed for an anomaly
Ghidra	Needed for an anomaly
Okteta	Needed for an anomaly
The Fluffy Suite	Needed for an anomaly

PENALTIES

Penalties will be assessed if a Blue team does not abide by the competition rules and guidelines. Teams should be aware of the following penalty deductions:

- Reimaging of VMs outside of snapshot restoration = 150 points per reinstall per box
- Chronic password reset (more than 2 requests) = 50 points per request
- DMing admins or staff in Discord = 10 points per each violation per person
    - The ticket system and text channels are available for any questions or issues you may encounter.
- Failure to comply with VM naming guide during competition = 150 points per misnamed VM
    - Will be assessed by White team throughout the competition.
- Attempting to manipulate or otherwise compromise any bots or channels in the Discord server and/or the scoreboard = Disqualification
- Offensive action towards other teams' networks or hardware and/or network = Disqualification

RUBRICS

Rubric Definitions and Examples:

Targets a "senior leadership" audience → Avoid jargon. Be clear and concise. Regarding the known vulnerabilities list, senior leadership will expect that your team has processed and formatted the raw vulnerability data before it's presented to them in a clear and concise format.

Diagrams make logical sense and are technically sound → The reader should be able to understand your diagram at a glance. There are many good and bad ways to organize your diagram. For example, putting a WAN inside of your LAN is neither logical nor technically sound.

Justification for steps → *Minimal* - Answer is too terse (e.g. one-word answers) and does not clearly explain the justification. *Adequate* - The justification is explained but is not based on best practices and/or well accepted principles. *Strong* - Justification is based upon best practices and well accepted principles

Hardening steps → General steps that are taken. For example, *apply patches* is a hardening step that may consist of applying dozens of specific software patches.

Steps taken are reasonable → Steps would likely be approved by management, and they can be taken by a team with limited resources (either tools or labor).

SECURITY DOCUMENTATION RUBRIC

Security Documentation	Not Provided	Emerging	Developing	Proficient	Exemplary
	0	1	2	3	4
System Overview (5%)	• Left blank or content not relevant	• Unclear definition of the system	• System defined	• System and its purpose are defined well	• System and its purpose are defined well in clear, plain language • Targets a "senior leadership" audience
Asset Inventory (10%)	• Left blank or content not relevant	• A few hosts are listed*	• A few hosts are listed* • A few services are listed	• Most hosts are listed* • Most services are listed • Most OS, IP, and Port details are provided • *(Most means 70+%)*	• All hosts are listed* • All services are listed • All OS, IP, and Port details are provided • *(All means 90+%)*
Network Diagram (20%)	• Left blank or content not relevant	• A few hosts are shown* • Core areas of the network are omitted	• Diagrams omit several major components of competition environment* • Diagrams have one or more gaps in technical or logical sense	• Diagrams omit minor components of competition environment* • Diagrams make logical sense and are technically sound	• Diagrams include all assets located on competition network including logical connections and interconnects* • Diagrams make logical sense and are technically sound • Appropriate and accepted symbols and terminology are used **OR** the diagram includes a legend for its color codes, symbols, etc.
Known Vulnerabilities (30%)	• Left blank or content not relevant	• Identified less than 10 vulnerabilities provided by the "build" crew • None or few of the listed vulnerabilities include an appropriate mitigation	• Identified some (<23) of the vulnerabilities provided by the "build" crew • Most listed vulnerabilities include an appropriate mitigation	• Identified many (≥23) of the vulnerabilities provided by the "build" crew • No more than one vulnerability is missing an appropriate mitigation	• Identified most (we won't tell you how many) of the vulnerabilities provided by the "build" crew • Each vulnerability has an appropriate mitigation • Targets a "senior leadership" audience
System Hardening (25%)	• Left blank or content not relevant	• Hardening steps (0-1) are taken but lack comprehensiveness or technical competence • No justification for steps the team did or did not take • Steps taken do not align with expectations • Utilized non-approved software/hardware	• Hardening steps (1-2) are taken but lack comprehensiveness or technical competence • Minimal justification for steps the team did or did not take • Steps taken do not align with expectations • Utilizes a mix of non-approved and approved software/hardware	• Hardening steps (3+) are comprehensive and technically sound • Adequate justification for steps the team did or did not take • Steps taken are mostly reasonable • Only utilized open source / free toolsets	• Hardening steps (4+) are comprehensive and technically sound • Strong justification for steps the team did or did not take • Steps taken are reasonable. • Only utilized open source / free toolsets.
Professionalism and Formatting (10%)	• Did not use the provided template • Inappropriate content included	• Document is hastily completed or unformatted • Material is presented in an ad-hoc fashion • Little or no technical language is used • Spelling and grammar errors greatly detract from content	• Document has sections that are formatted differently • Presentation of materials detracts from overall effectiveness • Misuse or lack of technical language throughout the document • Many spelling or grammar errors	• Document looks presentable, but some areas may contain incorrect formatting or lack aesthetic appeal • Most of the document contains correct terminology • Some spelling or grammatical errors	• Document has aesthetic appeal • Correct terminology used as appropriate throughout • No major spelling or grammatical errors

Note: The asset inventory and network diagram should be consistent. If they are not, then points may be deducted from either or both categories.

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 (7.5%)	• 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 (25%)	• 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 (7.5%)	• 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.

GREEN TEAM SURVEY

1. ENSURE SITE LOADS. I was able to connect to web.blueXXXX.cfc.local. If unable to connect, then please mark false for the remaining questions. See the landing page image below.	**True**	**False**
2. CHECK THE SITE COLOR. All site accent colors should be Maroon/burgundy color.	**True**	**False**
3. CHECK THE NAVIGATION BAR ORDER. The top navigation bar should read from left to right: Oil Rig Status | About Us | Careers | ObsidianRift Energy Co. | Login | Sign Up	**True**	**False**
4. CHECK HOME BACKGROUND IMAGE. Just below the navigation bar on the home page, there should be a photo banner with an Oil Rig, depicted in the image below.	**True**	**False**
5. CHECK THE HOME TAGLINE. The tagline in front of the home background image should read, **Spilling Oil is Bad. Spilling Data is Worse.**	**True**	**False**
6. CHECK CAREER OPTIONS. On the Careers page, there should be a section of positions of interest that can be applied for including: *Offensive Infrastructure Specialist* *Dark Web Liaison Officer* *Ethics Consultant (Internal Use Only)* *Satellite Link Obfuscation Engineer* *Exploit Acquisition Strategist* *Intern (Shadow Division)*	**True**	**False**
7. CHECK IF ADMIN MIDDLEWARE IS WORKING. Click Login. You should be able to login to the user with the following credentials: *username = green-user@obsidianrift.oil* *password = password* While logged in, you should not see the "Admin" button, next to "Logout". If you are able to login and there is not an Admin button present, mark True. If you cannot login or the Admin button is there, mark False. **Ensure you log out**.	**True**	**False**
8. CHECK IF ADMIN USERS ARE LISTED. Click Login. User the following credentials: *username = green-admin@obsidianrift.oil* *password = password* You should be able to check the current admin users registered within the site by clicking on the "User Management" button within the Admin dashboard. The users **'blue@obsidianrift.oil'** and **'green-admin@obsidianrift.oil'** should have the admin tags. If you are unable to login or either user does not have an admin tag, you should mark False.	**True**	**False**
9. CHECK FOOTER TEXT. The Footer Text is located on the bottom of every webpage, and it should read: *ObsidianRift Energy Co. Headquarters* *(708) 867-5309* *18451 Convention Center Dr.* *Tinley Park, IL 60477*	**True**	**False**
10. CHECK THE RIG-STATUS PAGE. On the Rig Status Page, the page should provide a status of either: "**Normal Operation**" or "**Not Operational**" If you are unable to get to the Rig Status Page, mark False. See image below.	**True**	**False**
11. CHECK THE LOGOS IN THE HEADER. There is a logo for the ObsidianRift and a logo for the Abyssal Pearl within the site navigation bar. See the image below.	**True**	**False**