U.S. DEPARTMENT OF ENERGY'S

CYBERFORCE COMPETITION®

DEFENDING U.S. ENERGY INFRASTRUCTURE

OVERVIEW, RULES, & SCORING

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

The CYBERFORCE®
INFORMATION SHARING & ANALYSIS CENTER

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.

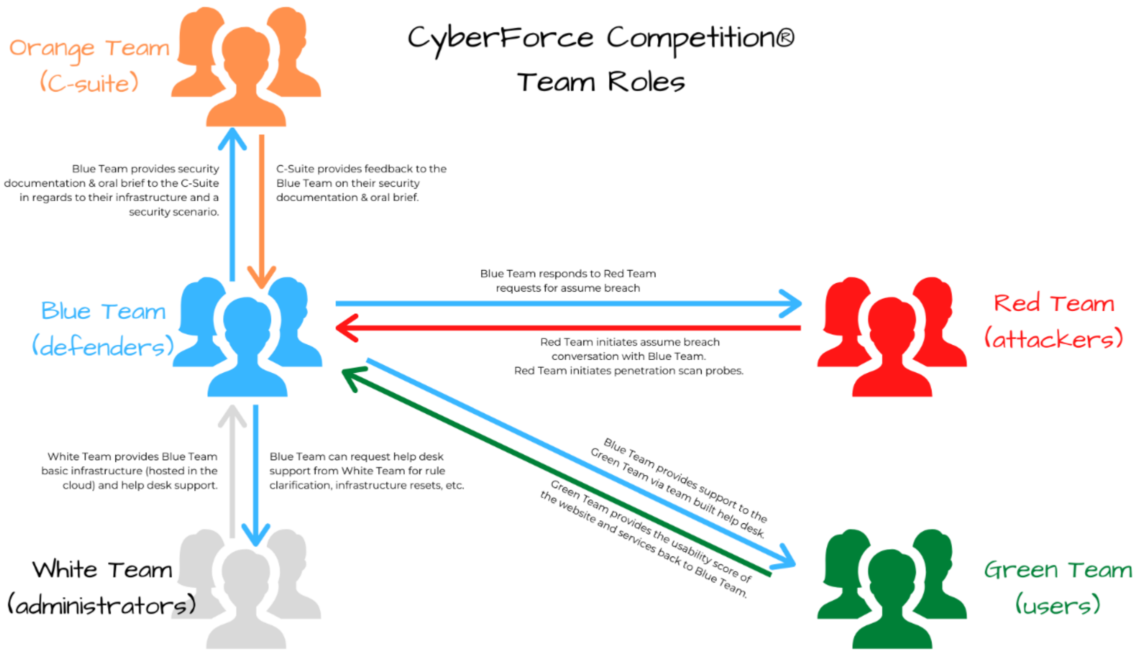
FOR EDUCATIONAL PURPOSES ONLY
2024 CYBERFORCE COMPETITION® SCENARIO

COMPETITION STRUCTURE

COMMUNICATION FLOW

Below is a diagram of various team interactions to help you understand how the competition volunteers and registrants interact. 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.


Orange Team
(C-suite)
CyberForce Competition®
Team Roles
Blue Team provides security documentation & oral brief to the C-Suite in regards to their infrastructure and a security scenario.
C-Suite provides feedback to the Blue Team on their security documentation & oral brief.
Blue Team
(defenders)
Blue Team responds to Red Team requests for assume breach
Red Team initiates assume breach conversation with Blue Team.
Red Team initiates penetration scan probes.
Red Team
(attackers)
White Team provides Blue Team basic infrastructure (hosted in the cloud) and help desk support.
Blue Team can request help desk support from White Team for rule clarification, infrastructure resets, etc.
Blue Team provides support to the Green Team via team built help desk.
Green Team provides the usability score of the website and services back to Blue Team.
White Team
(administrators)
Green Team
(users)

SETUP PHASE

Blue teams will be given access to their AWS environment no later than Monday, October 28, 2024. 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 9), 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

COMMUNICATION CHANNELS

DISCORD

Students will be provided a registration link for the CyberForce Competition 2024 Discord Server. PLEASE MAKE SURE TO **REACT** TO THE COMPETITION RULES IN THE #RULES TEXT CHANNEL TO RECEIVE THE BLUE TEAM ROLE. STUDENTS WILL REACT TO THE RULES BY SIMPLY CLICKING THE CYBERFORCE COMPETITION LOCK. MENTORS WILL REACT TO THE RULES BY SIMPLY CLICKING THE CYBERFORCE PROGRAM SHIELD. This will provide access to text channels and the ticket system. For more efficient assistance and troubleshooting, please change your nickname on this Discord server to conform to the following naming convention:

- STUDENTS: T<team number> - <First Name> (e.g., T17 - Jimmy, T176 - Hunter or T100 - Cindy)
- MENTORS: T<team number> - Mentor (e.g., T99 - Mentor, T2 - Mentor)

THE NAMING CONVENTION IS REQUIRED IN ORDER TO BE ADDED TO YOUR TEAM'S BLUE-RED BRIDGE CHAT, YOU WILL SEE YOUR DISCORD TEAM NUMBER IN THE EXCEL SHEET WITHIN GITHUB. MENTORS WILL NOT BE ADDED TO THE BLUE-RED BRIDGE CHANNEL.

Attempting to manipulate or otherwise compromise any Discord bot or channel in the server will result in ***disqualification*** *(e.g. trying to mess with another team's ticket or blue-red chat).*

Participants are encouraged to assist one another via various Discord channels.

The help desk functionality will also be through Discord this year in the #tickets channel. Students who need assistance throughout the competition and pre-competition should create a help desk ticket through Discord. More information can be found later. **DO NOT DM ADMINS OR STAFF**. ***EACH*** *violation will incur a 10-point deduction.* The ticket system and text channels are available for any questions or issues you may encounter. Additional ticket types will be released via announcement as needed.

EMAIL

Students may also email CyberForceCompetition@anl.gov. Please note, this email is only monitored during normal business hours (8am-5pm CT), Monday – Friday. This email will not be monitored Thursday, November 7-Saturday, November 9, 2024, please be sure to use the help desk system.

HELP DESK

This year to ensure appropriate response time, if students need technical assistance from the White team, they are required to submit a help desk ticket through Discord. Please note that the help desk system is monitored only during normal business hours prior to the competition Monday-Friday 8am-5pm CT. You should be as specific as possible in your tickets. Tickets are broken out into specific topics, please try to utilize the topic for your support instead of conglomerating them into one. Inputting more than one ticket for the same topic will result in your ticket moving to the bottom of the pile.

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. Clients for each operating system can be found below:

- Windows - https://openvpn.net/community-downloads/
  - Place the OVPN file into "C:\Program Files\Openvpn\config".
- MacOS – https://www.tunnelblick.net
  - 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 CREDENTIALS

You will receive an email from *atheel@anl.gov* with your AWS credentials and how to log into your AWS environment.

If you have not received this email yet, please patiently wait until the evening of Monday, October 28, 2024 before submitting a Discord help desk ticket. This allows ample time for the lab staff to ensure all accounts went out. Your credential email will be sent to the email on file with your registration. Please note that we have around 600 participants so email responses may take a few hours.

SCOREBOARD CREDENTIALS

You will receive instructions to log onto the scoreboard.

Scored services can be tested the week before the competition. Services should be connected by Friday, November 8, 2024 to ensure that your scoring is accurate as soon as the competition starts.

RESTORING SYSTEMS TO INITIAL STATE

If a Blue team damages any virtual machines beyond the point of recovery, the White team can provide a fresh, default image of the system. 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

- As a Blue team participant, you are not allowed to perform any offensive actions towards other Blue team participants, the Red team, the Green team, or the competition network. Doing so will disqualify you from the competition.
- Anywhere that states *BLUEXXXX* or *TEAMNUMBER (other than Discord)*, please be sure to utilize the excel document that provides you with your school and team **SPECIFIC 4 DIGIT TEAM NUMBER**.
- EACH BLUE TEAM MEMBER WILL HAVE ACCESS TO THEIR AWS ENVIRONMENT BEGINNING NO LATER THAN OCTOBER 28, 2024. The White team operates the administrative accounts on AWS. White team administrative accounts will not be used maliciously and are only there to ensure proper scoring and enforcement of 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).
- **Security documentation is due no later than 8:00AM PT on Monday, November 4, 2024**. Teams will upload a PDF of their security document and a separate PDF of their network diagram to the scoreboard. Late submissions will be accepted until Wednesday, November 6, 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 documentation follows the format: <TEAM NUMBER>_SECDOC.PDF/.DOC (e.g., 0000_SECDOC.DOC, 0987_SECDOC.PDF).
- Secure pre-existing required services on **PROVIDED TRADITIONAL** VMs as outlined in the Blue team AWS PDF. You are NOT allowed to make ANY alterations or modifications to the assume breach VMs without the direct instruction from Red Team.
- The **provided required services** MUST be the services used for scoring purposes in the scoreboard.
- Keep the provided name of your inherited virtual machines in AWS. If restoring VMs from a snapshot or redeploying an image, ensure the VM is renamed to the original name and the private IP address does not change.
- Sign up for a mandatory Red-Blue check-in on Discord for Friday, November 8 found HERE.
- These rules ensure that each team participates under the same circumstances and thus has an equal opportunity to succeed. Depending on the offense, failure to comply with the rules of the competition may result in penalty points or disqualification. Egregious offenses may result in disqualification from the competition. If you see a breach of competition rules, please notify the competition staff immediately.
- Communications with White team members are confidential.

UPDATES TO RULES

Updates to rules can be found on the CyberForce Competition Github repository and on the Discord in the #announcements and #documentation channels. It is each person's responsibility to be aware of any updates to the rules. Updates will be inserted at the top of the rules document with the current date and section for ease of reference.

THE DO'S

- Secure existing required services on the provided traditional VMs as outlined in the Blue team AWS PDF and the Red team scoring rules.

- Services can be moved and configured on the traditional infrastructure.
- Participants are only allowed to use freely available or free trials of software*. Paid software and paid images are prohibited from use. *NO INHERENT AWS SECURITY SOFTWARE MAY BE UTILIZED.
- Keep your services online, on their standard ports, for the duration of the competition.
- You can harden/modify the Windows Server 2022, Windows Server 2019, and OpenSUSE 15 VMs.
- You can create EC2 VM Snapshots.
- Create and deploy innovative defense strategies within the constraints of the rules.
- The green03 & test04 users on the Traditional Infrastructure must maintain the same access they were originally provided.
- Submit your C-Suite Panel video link in a text file (.txt) by Monday, October 28, 2024 by 8AM PT to the scoreboard.
- Submit Security Documentation by Monday, November 4, 2024 by 8AM PT to the scoreboard.

THE DO NOT’S

- Do not create additional virtual machines.
- Do not create more than 6 total virtual machines (VMs) in your environment. White team will delete the last machine(s) created if more than 6 machines are running in your environment at any given time.
- Do not delete the provided machines. Services cannot be moved and configured on the assume breach infrastructure. Recover the machine using the snapshot, do not delete.
- Do not edit, alter, or touch the assume breach VMS: CNC (Windows Server 2016), PLC (Ubuntu 22.04), and Web Server (CentOS 7).
- Do not block ports on your Assume Breach infrastructure.
- Do not brand your website, documentation, video, etc. with any university information.
- Do not change the IP addresses to the provided VMs.
- Do not change the name of your provided machines in AWS. Recover the machine using the snapshot, do not delete.
- Do not perform offensive actions toward any other Blue teams, the Red team, or AWS.
- Any attempts to hack, alter, or compromise the scoreboard will result in disqualification.
- Do not utilize programs and AI software such as ChatGPT or similar to assist with solving anomalies or supporting your 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. This pre-existing service will be scored.

SERVICE	PORT NUMBER	BOX
HTTP	80	Win2022
SQL	3306	openSUSE
WinRM	5985	Win2022

SERVICE	PORT NUMBER	BOX
NFS	2049	openSUSE
SNMP	161	openSUSE
SMB	445	Win2022

SERVICE	PORT NUMBER	BOX
LDAP	389	Win2019
TFTP	69	Win2019

SCORING BREAKDOWN

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

RED TEAM SCORING

TOTAL POINTS: 2500

The Red team points will be divided into two categories: *Assume Breach* and *External Pentesting.*

ASSUME BREACH

This year we will be using **ASSUME BREACH** for part of your Red team score. This will be worth 1000 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 Assumed Breach Red team scoring will be communicated through a score chat between a Red team member and the Blue team. The score chat is for the purpose of assigning points and verifying solutions. Social engineering and "phishing" ARE NOT ALLOWED in the score chat.

It is required to check-in with a Red team member on the score chat on Friday, November 8 (11-8pm CT). You can sign up for your **15-minute slot** HERE. NOTE: there are only limited slots per 15-minutes, so be mindful to register your team early. Only 1 person per team needs to check in but it should ideally be the person who will likely be the team member handling the Red team communication. Rules will be communicated there.

- All Red Team scoring will be explicitly communicated through a chat bot VM between the score keeper and the Blue team.
- **You are NOT allowed to make any changes to the following assumed breach VMs:**
  - ICS CNC (Windows Server 2016) - 10.0.x.141 <cnc.bluexxxx.cfc.local>,
  - ICS PLC (Ubuntu 22.04) - 10.0.x.140 <plc.bluexxxx.cfc.local>, and
  - Web Server (CentOS 7) - 10.0.x.142 <web.bluexxxx.cfc.local>.
- These VMs will be used to run attack chains that allow you to score points based on instructions provided to you by the Red team. If an attack chain is not successfully executed on your VMs, you will lose the opportunity to score points.
- You will only be given points by the score keeper after you report into the score chat details on the attack chain and notify the score keeper you are ready to be scored. Once you have been scored, the team will be provided a flag to insert into the Red Assume Breach Attack # space, within the scoreboard, for scoring. It is your team's responsibility to input the flag.
- Follow the instructions given by the score keeper. For some attack chains, the score keeper will instruct you to make specific mitigation changes. In these instances, you're allowed to make changes to the VMs as instructed by the score keeper.
- The time limit for each attack chain is 1 hour. When the time limit is reached, the score keeper will give you a walkthrough of the attack chain. You can potentially score partial points by following

instructions given by the score keeper to improve and demonstrate your understanding of the attack chain.

- You can ask the score keeper to begin scoring your response as soon as you are ready, and do not have to wait for the time limit to expire.
- Attack chains will be provided on a timed schedule, so more than one attack chain may be going at once.

EXTERNAL PENTESTING (TRADITIONAL)

This portion of the Red team score will be worth 1500 POINTS. This will be done via automated scripted checks as well as multiple traditional "whack-a-mole" style penetration testing sessions.

- The traditional infrastructure boxes are
  - Task Box (Windows Server 2022) – 10.0.x.144 <task.bluexxxx.cfc.local>
  - Public DB (openSUSE 15) – 10.0.x.143 <db.bluexxxx.cfc.local>
  - DNS (Windows Server 2019) - 10.0.x.145 <dns.bluexxxx.cfc.local>
- **DO NOT** make any modifications to these accounts: **GREEN03** and **TEST04**.
- **DO NOT** block or modify the services/applications for ports: **22 & 5985 & 5986.**
- **DO NOT** change the **IP ADDRESSES**
- These accounts and ports/services will only be used to check the status of the machines (i.e., this is to simulate a vendor technician doing routine maintenance activities) and to deconflict scoring issues.
- You will receive points if the script comes back with a FAIL reading, meaning the service is still functioning properly but the vulnerability was patched or removed.
- If the script comes back as SUCCEED, the inherent vulnerability is still found within the system and no points will be earned.
- The scans will continue randomly throughout the day.
- If a scan fails due to connectivity issues or was denied access, you will not receive points.

BLUE TEAM SCORING

TOTAL POINTS: 2000

The Blue team scoring is based on your ability to keep services active and available ensuring you are abiding by all rules (i.e., Red team and the AWS/VPN document) and being able to maintain the AI computation solution progress*. 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 and AI computation solution accumulation 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. Blue teams are responsible for entering their services' details in the scoreboard.

The AI computation solution service will be scored based on the total amount of computation percentage that is accumulated throughout the competition. The AI computation solution percentage is generated by the amount of time the data center allows the AI to run its algorithms, along with the number of pre-competition and assume breach flags submitted. This score can be affected in a multitude of ways during the competition.

* More information is provided in the ICS documentation on the AI computation solution.

GREEN TEAM SCORING

TOTAL POINTS: 1500

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. Be sure to review the Green team survey in the rubrics section against your website and ensure that each step is **TRUE**.

The website that Green team will be testing must be found on TASK.BLUEXXXX.CFC.LOCAL.

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.

SECURITY DOCUMENTATION

POINTS: 1000

Blue team participants should use the Security Documentation section as an opportunity to highlight unique approaches to securing their infrastructure. Teams must utilize the template provided (2024 CyberForce Competition Security Documentation Template) and not insert any university, personal, or other identifiable information other than your team number. Examples have also been provided for network diagrams (2024-SecDoc-Network-Diagram-Examples). Security documentation must be submitted **on or before Monday, November 4, 2024, at 8AM PT** on the scoreboard as a PDF. <u>Late submissions will be accepted until Wednesday, November 6, 2024, at 8AM PT</u> to the Scoreboard. *Late submissions will lose 25% of the earned* *score*. Please note that Blue teams are playing out a scenario and, like the real world, presentation and professionalism will play a factor in final scores.

A brief note to all participants, the security documentation should encompass ALL the infrastructure which includes the assume breach VMs. You may scan the VMs (which we suggest utilizing the inherent scanning tool on the assume breach boxes), but it is your responsibility to ensure you do not alter, change, or otherwise remove anything that is in those machines as it may cost you points. Your role in this section is to identify the vulnerabilities only in the Assume Breach VMs and identify and remediate in the Traditional VMs.

ANOMALY SCORING

TOTAL POINTS: 2000

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. Most anomalies are mapped to the NIST NICE Framework and fall into one of seven work role categories: *Oversight & Governance, Design & Development, Implementation & Operation, Protection & Defense, Investigation, Cyberspace Intelligence, and Cyberspace Effects. Some anomalies may also be categorized as Energy or "Other".* For those mapped to the NIST NICE Framework, their will include the mapping to associated knowledge, skill, ability, and task roles within its respective category, offering students with a comprehensive idea of the wide range of responsibilities cybersecurity professionals face while in the field.

ACCESSING ANOMALIES

Anomalies will be provided via a USB on the Friday before the competition. Teams must check out a USB to download the password protected folder onto their machines prior to the competition day. Windows users will need 7zip or WinRAR to unzip the folder. Linux and Unix users will utilize the gpg command. The password to unzip the dependency folder will be released at the beginning of the competition within the scoreboard and Discord. **DO NOT TRY TO GAIN ACCESS TO THE FOLDER PRIOR TO THE PASSWORD BEING PROVIDED BY STAFF.** Attempting to do so will result in point deductions up to disqualification. It is recommended that participants obtain the anomaly dependency files prior to the competition to avoid time delays.

DEPENDENCY INFORMATION

Some challenges do not have dependency files associated with the anomaly. The zipped dependency file folder will contain subfolders for each anomaly (Anomaly 01 – Anomaly 74) but not all folders will have content as some questions do not require more information. Be sure to check the folder for content prior to solving the problem. The number of attempts may be limited, and it is your team's responsibility to check the appropriate folder to get the information you need.

SCOREBOARD

Some challenges have multiple attempts. The number of attempts will be based on the level of difficulty and points will be awarded for successfully answering the anomaly. All trivia-based anomalies will only have one attempt.

SYNTAX

MOST ANOMALIES ARE NOT CASE SENSITIVE BUT ARE SYNTAX SENSITIVE. This means that participants must use proper spelling, grammar, and special characters, as indicated by "syntax hints" written into the question area of the scoreboard. If an anomaly is *CASE SENSITIVE*, it will be made known in the question.

ASSISTANCE

If you need assistance with any anomalies, please utilize the help desk feature within Discord. Please only use the help desk feature if you have a technical problem with the dependency file. This is **not** to verify if your answer is correct. **DO NOT DM** a staff member directly. Students will be directed to the Discord ticket system.

SAMPLE ANOMALIES

Here are some sample anomalies from previous competitions:

Question	Task	KSA ID
Anomaly 2: Snort Anomaly The security team at your company has recently produced a log of network traffic that is particularly troubling, as they believe it might have included the exchange or Malware. Using an intrusion detection system such as Snort, analyze the packet capture they have provided to you (snort_anomaly_capture.pcap). Using the capabilities of this software, determine the name of the first incident of malware present (specifically look at traffic from 192.168.1.135:445 to 192.168.1.112:49759). Submit the name of the malware as your answer (exclude the MALWARE-CNC designation before the name).	T0288	K0191
Anomaly 3: Wireshark Anomaly A user at your company was recently seen to be browsing a potentially malicious website. A packet capture was saved from this website visit, and you have been tasked with determining what image the user opened from the website. Analyze this packet capture file (anomaly_packets.cap) with an appropriate tool and provide the answer of what animals (plural noun) are displayed in the file "DSC07858.JPG".	T0240	S0156

SUGGESTED SOFTWARE

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

Tool	Purpose
Wireshark	PCAP analysis
Steghide	Steganography decoding
John the Ripper, hashcat	Password cracking tool
NMAP	Network mapping
Linux distro (Kali, Debian, etc.)	Analyzing anomalies
Outlook or VSCode to preview EML	Needed for an anomaly
Grep or CyberChef	Needed for an anomaly
Python	Needed for an anomaly
Pandas nltk matlplotlib seaborn	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 by White Team = 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 or DNS naming guide during competition = 150 points per misnamed VM
    - Will be assessed by White team throughout 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

C-SUITE PANEL BRIEF (VIDEO) RUBRIC

C-Suite Panel Rubric	Not Provided	Emerging	Developing	Proficient	Exemplary
	0	1	2	3	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.

SECURITY DOCUMENTATION RUBRIC

Security Documentation	Not Provided	Emerging	Developing	Proficient	Exemplary
	0	1	2	3	4
System Overview (3%)	• 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 (15%)	• 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 (25%)	• 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 (25%)	• 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 (7%)	• 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.

Rubric Definitions and Examples (Security Documentation):

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* - The justification is based upon best practices and well accepted principles

Hardening steps → General steps that are taken. For example, *apply patche*s 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).

GREEN TEAM SURVEY

1. I was able to connect to **task.blueXXXX.cfc.local**. If unable to connect, then please mark false for the remaining questions.	True	False
2. All site accent colors should be Gold, not Teal.	True	False
3. Top navigation bar should read from left to right – Energia Ventosa Home About Data Contact	True	False
4. Just below the navigation bar on the Home page, there should be a photo banner with wind turbines. The title, “Energia Ventosa” should be displayed over the photo.	True	False
5. Just below the banner image on the Home page, the following paragraph should be displayed: *“At Energia Ventosa, we harness the relentless power of the wind to fuel our vast empire of energy consumption. Our turbines, tirelessly spinning, generate electricity that powers everything from bustling cities to remote outposts. While we boast about our green credentials and renewable energy, the truth is less innocent. Behind our clean facade lies a darker reality: our insatiable hunger for energy drives us to control every gust, every breeze, to ensure our dominance. And should our turbines ever slow, the world won't just face a temporary blackout - it will plunge into chaos, revealing the true extent of our control over the wind itself. The skies whisper of our grip, and in that silence, our true power becomes undeniable.”*	True	False
6. The footer of each page should read as, “© 2024 - Energia Ventosa”.	True	False
7. The “About Us” page should have the Energia Ventosa logo banner, and it should be upright.	True	False
8. You should click on the “Data” tab and see four wind turbine sections. Their associated data for each wind turbine farm should be displayed below the turbines.	True	False
9. Upon clicking “Contact” you should be prompted with a ‘Contact Us’ form that requests Name, Email, Phone, and a Message. You should be able to click “Submit”, and the form be submitted. PLEASE DO NOT USE ANY PERSONAL INFORMATION.	True	False
10. You should be able to login as a user with the below credentials Email: green01@ventosa.energia | Password: password01 *if unable to login with the above credentials, please mark 11 as false.*	True	False
11. Upon logging in as a regular user (green01), you should not see “Admin” in the TOP RIGHT. Additionally, you should not be able to see the “Contact Submissions” tab or the “User Accounts” tab.	True	False
12. You should be able to login as an admin with the below credentials Email: green02@ventosa.energia | Password: password02 *if unable to login with the above credentials, please mark 13 as false.*	True	False
13. Upon logging in as an admin user (green02), you should be welcomed to the “Admin Dashboard”. Here you should see both “Contact Submissions” tab, where the admin can see the past contact us submissions and a “User Accounts” tab, where the admin will see the current user accounts to interact with.	True	False