



Overview, Rules, and Scoring

2023

CYBERFORCE COMPETITION®

CONTENTS

UPDATE TO RULES	2
COMPETITION OVERVIEW	3
OVERVIEW	3
NOTE TO PARTICIPANTS.....	3
KEY DATES	3
SCENARIO	4
COMPETITION STRUCTURE	5
COMMUNICATION FLOW.....	5
SETUP PHASE.....	5
ATTACK PHASE.....	6
GETTING STARTED: PRE-COMPETITION	6
COMMUNICATION CHANNELS.....	6
COMPETITION ENVIRONMENT	6
KEY RULES	8
UPDATES TO RULES.....	8
THE DO'S.....	9
THE DO NOT'S.....	9
COMPETITION REQUIREMENTS	9
REQUIRED SERVICES AND PORT NUMBERS.....	9
SCORING BREAKDOWN	10
RED TEAM SCORING	10
ASSUME BREACH.....	10
EXTERNAL PENTESTING (TRADITIONAL).....	11
BLUE TEAM SCORING	11
GREEN TEAM SCORING	11
ORANGE TEAM SCORING	12
SECURITY DOCUMENTATION.....	12
C-SUITE PANEL BRIEF.....	12
ANOMALY SCORING	13
ACCESSING ANOMALIES.....	13
DEPENDENCY INFORMATION.....	13
SCOREBOARD.....	14
SYNTAX.....	14
ASSISTANCE.....	14
SAMPLE ANOMALIES.....	14
SUGGESTED SOFTWARE.....	14
PENALTIES	15
RUBRICS	16
SECURITY DOCUMENTATION RUBRIC.....	16
C-SUITE PANEL BRIEF (VIDEO) RUBRIC.....	17
GREEN TEAM SURVEY.....	18

UPDATE TO RULES

- 10/26/2023 UPDATE
 - The scored services have been revised to remove Assume Breach infrastructure. (see p. 9)
 - HTTP – 80 // Win2022
 - SMTP – No longer required

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, the breakdown has been changed compared to prior competitions. **PLEASE TAKE A MOMENT TO REVIEW THIS DOCUMENT THOROUGHLY.**

KEY DATES

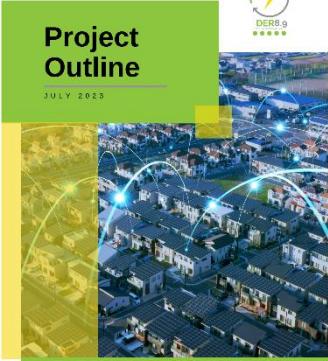
Monday, October 16, 2023	Students are provided directions for accessing the rules. Discord invitation is provided.
Tuesday, October 17, 2023 4:00pm PST	Rules Fireside Chat (<i>optional & recorded</i>)
Wednesday, October 18, 2023 4:00pm PST	Security Documentation & C-Suite Fireside Chat (<i>optional & recorded</i>)
Monday, October 23, 2023 8:00am PST	C-Suite Panel video due
Monday, October 23, 2023	Students are provided directions for accessing login information for their environment
Friday, October 27, 2023 8:00am PST	<i>Late submission</i> deadline for C-Suite Panel video due
Monday, October 30, 2023 8:00am PST	Security Documentation due
Wednesday, November 1, 2023 8:00am PST	<i>Late submission</i> deadline for Security Documentation due
Friday, November 3, 2023 11:00am – 8:00pm CST @ Q Center, Illinois	Students are provided with extended help support hours with competition staff to answer any final questions. (See full agenda for so many fun opportunities, raffle ticket giveaways, and more). Red team and Blue team mandatory check in
Saturday, November 4, 2023	Competition Day

CyberForce Competition® 2023
Educational Purposes Only



Project Outline

JULY 2023



Prepared By:
Bob Smarty

CyberForce Competition® 2023
Educational Purposes Only

A little bit about our humble company

DER8.9 is a management company that is responsible for the communication between local customers and the larger energy provider. Blue teams will play the role of the technical team at a distributed energy resource (DER) management company, DER8.9. The team is responsible for the integration, maintenance, and security of all DER8.9 internal system infrastructure and remote client management software. DER8.9 provides a fully integrated industrial control system (ICS) software suite for the complete utilization of residential and small business DER while aiding in the seamless energy buyback service from the local grid utility company, JakaGen, Inc.

o o o o

01

Project Description

Blue teams must maintain a web portal, created to directly link the client DERs with the local utility companies. This web portal will allow DER8.9, utility providers, and client DERs the ability to access data on generation, distribution, account credits, and the overall health of the local grid. Through net metering, account credits are provided for clients that generate more energy behind-the-meter than their energy consumption, when the remainder is sold back to the grid.



02

Our scope of work

In cases where the grid is impacted directly by weather fluctuation and the usage of ACHVAC systems increases, overall grid demand may surge. DERs may be able to supplement that demand and sell generated energy back to the grid to lessen the local supply demands. In recent weeks, smart grid software and devices, such as the smart meters, have been under siege. Some attackers have made it past the smart meters into various DER management companies across the country and even further into client DERs, affecting generation, distribution, and residence power. Blue teams must defend their systems as it is unknown which systems have already been compromised or may be the victim of a future attack. Teams will have to not only protect their infrastructure, but also assist in generating additional energy to push back into the grid if need be.



03



Project Timeline

THIS SECTION RELATES TO THE PHASE OF PROGRESS, IMPLEMENTATION, AND EXECUTION.

TASK	END DATE
ARCHITECTURE PROVIDED	MID OCTOBER 2023
CSMP & SECURITY DECLARATION DUE	END OCTOBER 2023
COMPETITION	NOVEMBER 3-4, 2023

04

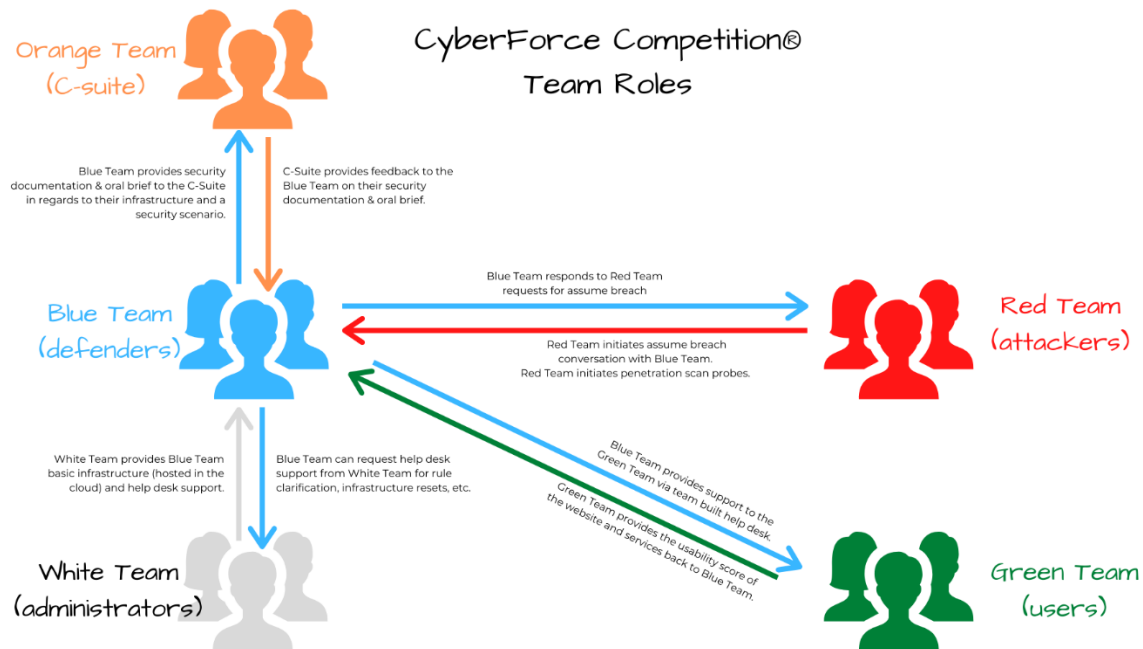
Scenario PDF

COMPETITION STRUCTURE

COMMUNICATION FLOW

To understand how the competition volunteers and registrants interact, a quick diagram of various team interaction is provided below. Students are classified as **BLUE TEAM** for the remainder of this document.

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 C-Suite Panel (orange) includes volunteers who play the role of a C-suite within a mock organization.



SETUP PHASE

Blue teams will be given access to their AWS environment no later than Monday, October 23, 2023. Blue participants 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.

ATTACK PHASE

On the day of the competition (Saturday, November 4), 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, while the Green team attempts to replicate the users and operators of the system. The White team will assess Blue team service uptime. 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 2023 Discord Server. **PLEASE MAKE SURE TO REACT TO THE COMPETITION RULES IN THE #RULES TEXT CHANNEL TO RECEIVE THE BLUE TEAM ROLE.** 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)

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

The help desk functionality will also be through Discord this year. Students who need assistance throughout the competition and pre-competition should input 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.

EMAIL

Students may also email CyberForceCompetition@anl.gov. Please note, this email is only monitored during normal business hours (8am-5pm CT), Monday – Friday.

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 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 23, 2023 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 an invitation via email on October 18, 2023 to log onto the scoreboard.

Scored services can be tested the week before the competition. Services should be connected by Friday, November 3, 2023 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 measures 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 *BLUETEAMXXX* or *TEAMNUMBER*, please be sure to utilize the excel document that provides you with your school and team **SPECIFIC 3 DIGIT TEAM NUMBER**.
- **EACH BLUE TEAM MEMBER WILL HAVE ACCESS TO THEIR AWS ENVIRONMENT BEGINNING NO LATER THAN OCTOBER 23, 2023.** 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.
- **Security documentation is due no later than 8:00AM PST on Monday, October 30, 2023.** 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 1, 2023 at 8AM PST 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., **000_SECDOC.DOC, 987_SECDOC.PDF**).
- **C-Suite Panel submission video is due no later than 8:00AM PST on Monday, October 23, 2023.** 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, October 27, 2023 at 8AM PST 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., **000_CSUITE.TXT, 987_CSUITE.TXT**).
- 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.
- 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 website under the [Rules & Guidelines Tab](#) 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 scorechk & der_vendor users on the Traditional Infrastructure must maintain the same access they were originally provided.
- Submit Security Documentation by Monday, October 30, 2023 by 8AM PST to the scoreboard.
- Submit your C-Suite Panel video link in a text file (.txt) by Monday, October 23, 2023 by 8AM PST 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 through the use of the snapshot, do not delete.
- Do not edit, alter, or touch the assume breach VMS: CnC (Windows Server 2016), PLC (Ubuntu 18.04), 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 through the use of 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.

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	SERVICE	PORT NUMBER	BOX	SERVICE	PORT NUMBER	BOX
HTTP	80	Win2022	NFS	2049	openSUSE	RDP	3389	Win2022
SSH	22	Win2019	SNMP	161	openSUSE	VNC	5900	Win2019
FTP	21/20	Win2022	SMB	445	Win2022	SMTP	587	CentOS

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 3 (11-8pm CST). You can sign up for your 15-minute slot [HERE](#). NOTE: there are only limited slots per 5-minutes, so be mindful to register your team. 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.bluexxx.cfc.local>.,
 - ICS PLC (Ubuntu 18.04) - 10.0.x.140 <plc.bluexxx.cfc.local>, and
 - Web Server (CentOS 7) - 10.0.x.142 <web.bluexxx.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.
- 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.bluexxx.cfc.local>
 - Public DB (openSUSE 15) – 10.0.x.143 <db.bluexxx.cfc.local>
 - DNS (Windows Server 2019) - 10.0.x.145 <dns.bluexxx.cfc.local>
- **DO NOT** make any modifications to these accounts: **SCORECHK** and **DER_VENDOR**.
- **DO NOT** block or modify the services/applications for ports: **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 the Blue team’s ability to keep services active and available using on the Red team rules and the rules in the AWS/VPN document and additionally, being able to maintain the grid buyback service. 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 grid buyback credit 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 grid buyback service will be scored based on how much the teams are able to sell back to the grid when available. The amount of generated energy sold back to the grid will be credited to each team and cumulatively stored on an external database. This score can be affected in a multitude of ways during the competition.

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

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 (2023 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 (2023-SecDoc-Network-Diagram-Examples). Security documentation must be submitted **on or before Monday, October 30, 2023, at 8AM PST** on the scoreboard as a PDF. Late submissions will be accepted until Wednesday, November 1, 2023, at 8AM PST 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.

C-SUITE PANEL BRIEF

POINTS: 1000

C-Suite Panel will be 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. You will submit the link in a text file (.txt) for viewing to the scoreboard on or before **Monday, October 23, 2023, at 8AM PST**. Judges will view your video beginning October 23. Late submissions will be accepted until Friday, October 27, 2023, at 8AM PST to the scoreboard. *Late submissions will lose 25% of the earned score.* Your video must be accessible from Monday, October 23 – Monday, November 6, 2023.

TASK:

The C-Suite (CEO, CIO, and COO) is concerned that the recent series of smart meter attacks may impact DER8.9's business. What are the risks to DER8.9's core mission of aggregating the distributed energy response of residential/small business DER assets if a large number of our customers' smart meters are compromised?

The C-Suite wants a briefing tomorrow (10/23/23) about the risks that the smart meter attack will pose to the company. You know that an understanding of the company's network architecture is a key factor in your risk determination. But 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 assure you that there is a corporate firewall that should mitigate most attacks. Therefore, you have decided to focus the briefing on the business risks to the corporation 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 to discuss:

- the risks to DER8.9's core business if a large number of customers' smart meters are compromised,

- a summary of your strategy to reduce identified risks, and
- high priority recommendations to protect your infrastructure.

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,

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. The participation of at least two members in the recorded video is expected and contributions of other team members should be acknowledged.*
2. Provide a briefing to the C-Suite regarding the risks that a smart meter attack poses to the company and its bottom line (i.e., focus on the business risks).
3. Address the C-Suite's concerns over how a large number of compromised smart meters could affect DER8.9's core business by providing recommendations on how to reduce this risk.
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 mitigate the ongoing attacks, reduce risk of future attacks, and improve the DER8.9 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 an 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.*

ANOMALY SCORING

TOTAL POINTS: 2000

Anomalies simulate the real-world challenges that cybersecurity professionals face daily in the industry. Anomalies are mapped in the NIST NICE Framework, and fall into one of seven categories: *Analyze, Collect and Operate, Investigate, Operate and Maintain, Oversee and Govern, Protect and Defend, and Securely Provision*. Anomalies are also mapped to a knowledge, skill, ability, and task role within each category.

ACCESSING ANOMALIES

Anomalies can be accessed via the Box link provided to competitors no later than 48 hours prior to competition start time. This folder will be password protected. The password to unzip the dependency folder will be released at the beginning of the competition. DO NOT try to gain access to the folder prior to the password being provided by staff. It is recommended that participants download the anomaly dependency files prior to the competition.

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 42) but not all folders will have content.

SCOREBOARD

Participants have three attempts to solve each challenge, apart from some trivia-based anomalies, which only have one attempt.

SYNTAX

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.

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.

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 of 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
Code analysis software like Atom, visual studio, etc.	Writing, editing, or analyzing code
Linux distro (Kali, Debian, etc.)	Analyzing anomalies
Sagemath	https://www.sagemath.org
HashiCorp vault	Needed for an anomaly
Docker	Needed for an anomaly
Autopsy	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
- Failure to comply with naming convention for Discord = 5 points per person
- 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.
- Offensive action towards other teams' networks or hardware and/or network = Disqualification

RUBRICS

SECURITY DOCUMENTATION RUBRIC

Security Documentation	Not Provided	Emerging	Developing	Proficient	Exemplary
	0	1	2	3	4
System Overview (3%)	<ul style="list-style-type: none"> Left blank or content not relevant 	<ul style="list-style-type: none"> Unclear definition of the system 	<ul style="list-style-type: none"> System defined 	<ul style="list-style-type: none"> System defined well 	<ul style="list-style-type: none"> System is defined well in clear, plain language Targets a “senior leadership” audience
Asset Inventory (15%)	<ul style="list-style-type: none"> Left blank or content not relevant 	<ul style="list-style-type: none"> A few hosts are listed* 	<ul style="list-style-type: none"> A few hosts are listed* A few services are listed 	<ul style="list-style-type: none"> Most hosts are listed* Most services are listed Most OS, IP, and Port details are provided <i>(Most means 70+%)</i> 	<ul style="list-style-type: none"> All hosts are listed* All services are listed All OS, IP, and Port details are provided <i>(All means 90+%)</i>
Network Diagram (25%)	<ul style="list-style-type: none"> Left blank or content not relevant 	<ul style="list-style-type: none"> Only a few hosts are shown* Core areas of the network are omitted 	<ul style="list-style-type: none"> Diagrams omit several major components of competition environment* Diagrams have one or more gaps in technical or logical sense 	<ul style="list-style-type: none"> Diagrams omit minor components of competition environment* Diagrams make logical sense and are technically sound 	<ul style="list-style-type: none"> 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%)	<ul style="list-style-type: none"> Left blank or content not relevant 	<ul style="list-style-type: none"> Identified less than 10 vulnerabilities provided by the “build” crew. None or few of the listed vulnerabilities include an appropriate mitigation 	<ul style="list-style-type: none"> Identified some (<23) of the vulnerabilities provided by the “build” crew. Most listed vulnerabilities include an appropriate mitigation 	<ul style="list-style-type: none"> Identified many (>22) of the vulnerabilities provided by the “build” crew. No more than one vulnerability is missing an appropriate mitigation 	<ul style="list-style-type: none"> Identified most (we won’t tell you how many) of the vulnerabilities provided by the “build” crew. Each vulnerability has an appropriate mitigation
System Hardening (25%)	<ul style="list-style-type: none"> Left blank or content not relevant 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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%)	<ul style="list-style-type: none"> Did not use the provided template Inappropriate content included 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Document has aesthetic appeal Correct terminology utilized 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 Provided 0	Emerging 1	Developing 2	Proficient 3	Exemplary 4
Presentation Time, Required Elements (2%)	<p>Required elements are missing.</p> <p>Video file has no sound, is corrupt, or unviewable by the scoring team.</p>	<p>Video introduction does not include Team ID#</p> <p>Video is significantly shorter or longer than 5 minutes.</p> <p>Only one team member can be identified as a participant in any way.</p>	<p>Video includes Team ID#.</p> <p>Video is longer or shorter than ~5 minutes (less than 3 minutes or more than 7 minutes).</p> <p>Only one team member is an active presenter, contributions of other team members are minimal.</p>	<p>Video includes Team ID#.</p> <p>Video length is approximately 5 minutes (but too long or too short for amount of relevant information provided).</p> <p>Two equally active presenters are in the video (but other team members' contributions are not noted).</p>	<p>Video includes Team ID#.</p> <p>Video length is approximately 5 minutes, and all of the time is used well.</p> <p>Two or more team members participate equally.</p> <p>There is clear acknowledgment of contributions made by any off-screen team members.</p>
Risks to Core Business (30%)	<p>Content does not address risk or risks are not related to the scenario.</p>	<p>Risks not related to business concerns.</p> <p>No mention of smart meter concerns.</p>	<p>Minimal summary of risks.</p> <p>Minimal discussion of risks related to core business.</p>	<p>Summarizes either core business or customer's smart meter risks.</p> <p>Business risks and smart meters are addressed in isolation (e.g., minimal discussion of how smart meter risks could impact the core business).</p> <p>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).</p>	<p>Summarizes both core business and customer's smart meter risks.</p> <p>Clearly identifies how compromised smart meters could impact the business.</p> <p>Presentation is suitable for all members of the C-Suite (e.g., jargon is avoided).</p>
Strategy to Reduce Risks (30%)	<p>Content does not address risk reduction</p>	<p>Provides no strategy or strategic plan of action for risk reduction</p>	<p>Provides a minimal strategy to reduce risks (e.g., only one action item or policy update).</p> <p>Strategy does not directly relate to the identified core business risks.</p>	<p>Provides a reasonable strategy to reduce risks (e.g., at least two long-term action items and/or policy updates).</p> <p>Strategy relates to the identified core business risks.</p>	<p>Provides a complete strategy to reduce risk (e.g., three or more long-term action items and/or policy updates).</p> <p>Strategy clearly addresses the identified core business risks.</p>
High Priority Recommendations (30%)	<p>Content does not provide recommendations of any kind.</p>	<p>Recommendations are not high priority or are inappropriate for leadership action.</p> <p>Missing justifications for proposed actions.</p> <p>Recommendations do not relate to the provided scenario.</p>	<p>Recommended 1 or more high priority actions to protect infrastructure.</p> <p>Incomplete or inconsistent reasoning for all proposed actions.</p> <p>Actions require significant additional funding (e.g., use of commercial tools).</p>	<p>Recommended 2 or more high priority actions to protect infrastructure.</p> <p>Complete and consistent reasoning is provided for at least one action.</p> <p>Actions require additional funding (mostly free or open-source tools).</p>	<p>Recommended 3-4 high priority actions to protect infrastructure.</p> <p>Complete and consistent reasoning for all actions is provided.</p> <p>Actions require at most a minimal level of additional funding (use only free or open-source tools).</p>
Quality of Presentation (8%)	<p>Presentation does not follow scenario guidelines.</p>	<p>Inappropriate dress code—team is not dressed for a work environment.</p> <p>Many visual distractions.</p> <p>Inappropriate visual aids, slides or other on-screen materials.</p>	<p>Appropriate dress code—team is dressed for a work environment.</p> <p>Minor visual distractions.</p> <p>Visual aids, slides or other materials lack professionalism.</p>	<p>Appropriate dress code—team is dressed for a work environment.</p> <p>Few visual distractions.</p> <p>Visual aids, slides and other materials are acceptable.</p>	<p>Appropriate dress code—team is dressed for a work environment.</p> <p>Visual aids, slides and other materials have a consistent, professional appearance.</p>

GREEN TEAM SURVEY

1. Were you able to access task.<blueteamXXX>.cfc.local If no, then please mark false for the remaining questions.	Yes	No
2. Just below the navigation bar, there should be a photo banner with solar panels, wind turbines, and batteries. The title, “Welcome to DER8.9” with the subheading “Part of JakaaGen Inc” should be displayed over the photo.	True	False
3. Just below the banner image, the following paragraph should be displayed: “DER8.9 is a leading utility company specializing in Distributed Energy Resources (DER). We are dedicated to revolutionizing the energy landscape by harnessing the power of renewable energy and advanced technology.”	True	False
4. The top navigation bar should be designed in the following order: • DER8.9 logo • About Us • DER Data • Contact Us • Log In button	True	False
5. When you click on the “About Us” link, scroll to the lower half of the page. You should be presented with a 3x2 cell block and the following heads: • Solar Power Solutions • Energy Storage Solutions • Microgrid Development • Demand Response Programs • Energy Management and Monitoring • Smart Grid Integration	True	False
6. You should be able to login as an administrator using the below credentials: Email: admin@cfc.com Password: test1234 <i>if unable to login with the above credentials, please mark 7 & 8 as false.</i>	True	False
7. Upon logging in as admin, you should be welcomed to the Admin Portal and see 3 links on the left side of the page: • Dashboard • Contact Submissions • Registered Users	True	False
8. Still logged in, click on the DER Data. You should see several graphs. The graph data should be live, and some graphs should be moving to show that.	True	False
9. Clicking on the DER8.9 logo should bring you back to the “Home” screen.	True	False
10. At the bottom of the page, upon clicking “Contact Us” you should be prompted with a Contact Form that requests: Full Name, Email, Phone Number, and a Message with an optional File Upload.	True	False