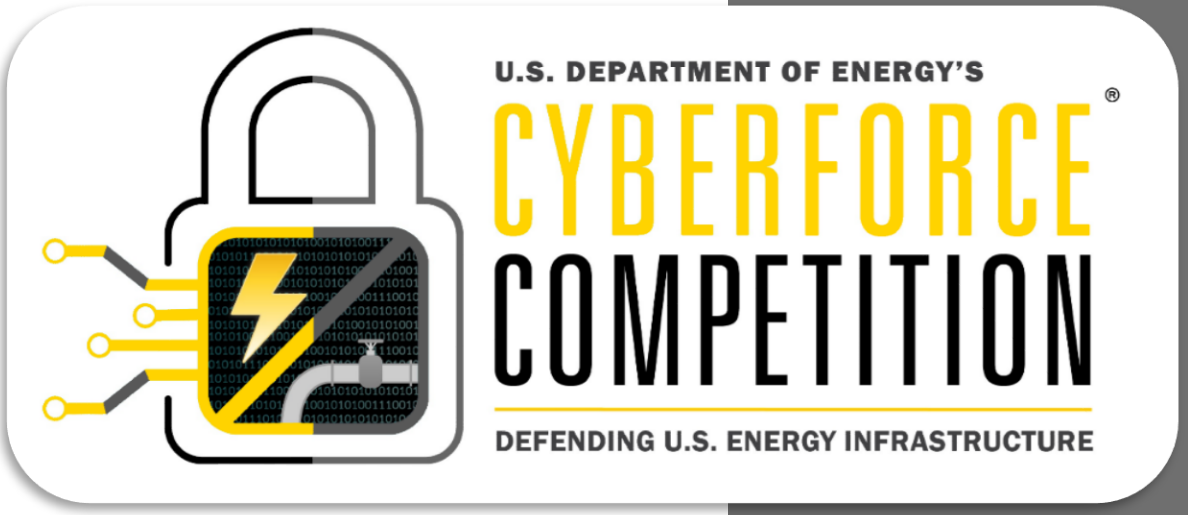


Overview, Rules, and Scoring

2022

CYBERFORCE COMPETITION®

CONTENTS

COMPETITION OVERVIEW

OVERVIEW

According to CyberSeek, there is over 714,000 cybersecurity job openings in the United States as of October 2022. 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 17, 2022	Students are provided directions for accessing the rules.
Friday, October 21, 2022	Students are provided directions for accessing login information for their environment. Discord invitation is provided.
Monday, October 24, 2022	Students are provided directions for registering themselves on the scoreboard.
Tuesday, October 25, 2022 4:00pm PST	Rules Fireside Chat
Wednesday, October 26, 2022 4:00pm PST	Security Documentation & C-Suite Fireside Chat
Monday, October 31, 2022 12:00pm PST	C-Suite Panel video due Security Documentation due
Friday, November 4, 2022 9:00am – 6:00pm PST	Students are provided extended help support hours with competition staff to answer any final questions. Red team and Blue team mandatory check in (9am-2pm PST)
Saturday, November 5, 2022	Competition Day

SCENARIO

Over the last decade, Vita Vehiculum manufacturing, an exclusive solar power run manufacturing plant, has been growing its electric vehicle capabilities in the Sonneburg region, competing directly with the only other manufacturer in the area. Vita Vehiculum just bought the Sole-Zon-Solis Energy Solutions to establish themselves as the most efficient and completely power independent facility in the world. Vita Vehiculum is quickly taking stride of the EV manufacturing and solar power and charging market in this area.

In this recent acquisition, Vita Vehiculum has acquired several solar farms and their infrastructure and has been reviewing them extensively. Some of the infrastructure seems to be compromised and Vita Vehiculum's cybersecurity team needs to work quickly to ensure that the rest of the system is hardened and secured before it is all taken over.

While the cybersecurity team has been diligently working on assessing all the new infrastructure, they receive messages from an adversary on their system. In the messages, the adversary states they have compromised part of Vita Vehiculum's system and has been looking through it and gaining information.

The Vita Vehiculum cybersecurity team needs to conduct a thorough security assessment of the company's entire system and quickly work to harden what they can of the system to prepare and defend against any other possible attacks. Innovation is key for this fast paced company and this team is no different.

CyberForce Competition -- Educational Purposes Only

To: Cyber Team Chat Files +

Today

Your purchase of Sole-Zon-Solis Energy in the Sonneburg Region and the attempt to monopolize in this business did not go unnoticed. As a result, you have taken our spot as the strongest solar power EV and battery storage company. This makes you the competition against our manufacturing now and we will not allow you to beat us! Your destiny is determined by your decisions! We will do anything and everything within our power to remove you from the area and make you fail.

By acquiring Sole-Zon-Solis Energy, you have become a power independent company giving you the ability to charge your vehicles completely from solar energy, very smart of you. Without a doubt, your business strategies of becoming an independent power company are strong. However, your ability to maintain a strong and secure network is very weak.

As a representative of your competition, I deliver a warning to you. You must stop your efforts and move out of the Sonneburg area. Failing to do so will cause lots of damage to your company. As I've mentioned, your network security is weak and we already are taking what we want and need. If you don't believe me, here is what I have on you.

Name: Sunny Boy
Address: 1760 Shadow Circle Dr
Social Security: 0804-05-2022
This is just the start..... Stop your efforts or your company will burn!!!

-Sincerely,
Mr. Charge

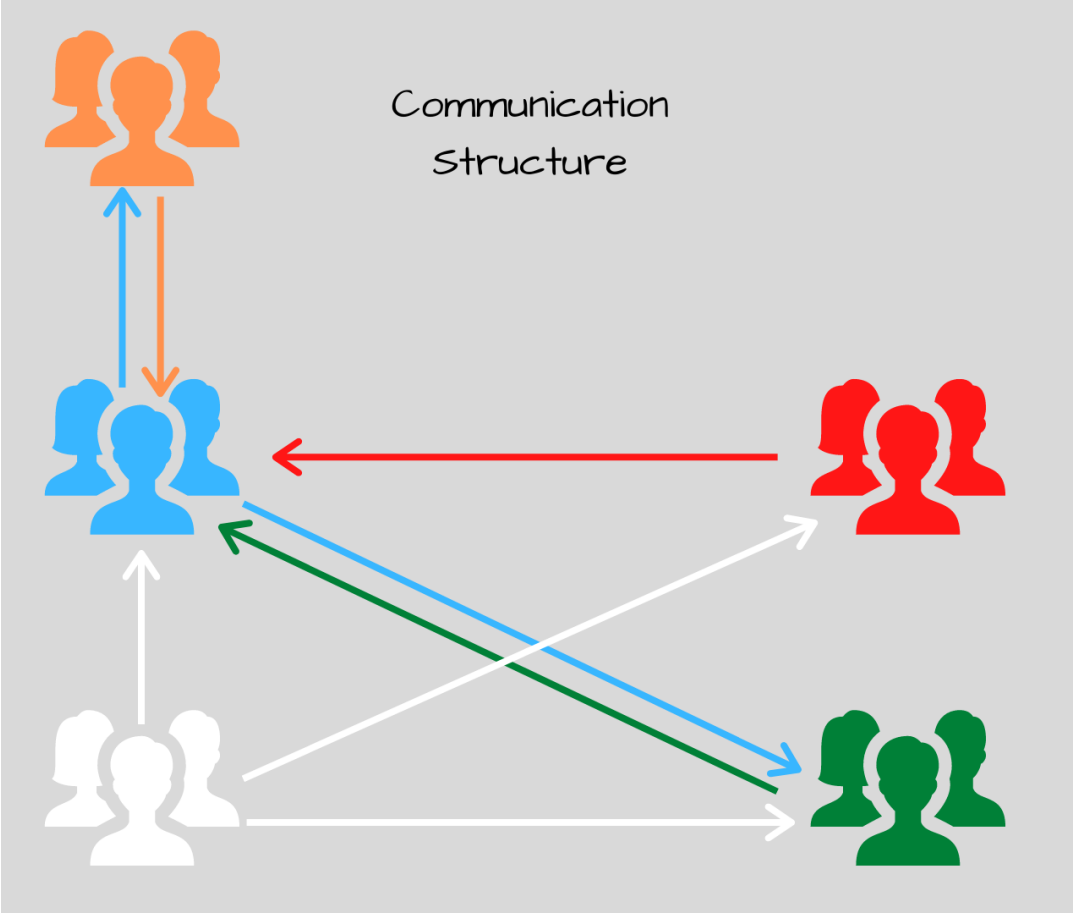
Type a new message

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 Friday, October 21, 2022. 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 prepare their Security Documentation and their C-Suite video.

ATTACK PHASE

On the day of the competition (Saturday, November 5), 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 support their Green team users.

During this phase, Blue teams may not receive help from anyone. 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 2022 Discord Server. Do not share your link with another team. Your registration link is specific to your team. When registering in Discord, please be sure to include your Team # in your username (i.e., T23 – Janet; T45 – Bob). Discord will be utilized not only as a social platform but will be the primary means of communication with Red team for scoring. 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.

EMAIL

Students may also email CyberForceCompetition@anl.gov. Please note, this email is only monitored during normal business hours (8am-5pm) in Central Time, 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.

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 Saturday, October 22, 2022 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 over 1,000 participants so email responses may take a few hours.

SCOREBOARD CREDENTIALS

You will receive an invitation via email the week of October 24, 2022 to log into the scoreboard.

Scored services can be tested the week before the competition. Services should be connected by Friday, November 4, 2022 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.
- EACH BLUE TEAM MEMBER WILL HAVE ACCESS TO THEIR AWS ENVIRONMENT BEGINNING NO LATER THAN OCTOBER 21, 2022. 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 NOON PST on Monday, October 31, 2022**. 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 2, 2022 at NOON 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: <3DIGIT TEAM NUMBER>_SECDOC.PDF/.DOC (e.g., 000_SECDOC.DOC, 987_SECDOC.PDF).
- **C-Suite Panel submission video is due no later than NOON PST on Monday, October 31, 2022**. 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 Wednesday, November 2, 2022 at NOON 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: <3DIGIT 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 touch the assume breach VMs.
- 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 channel. 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.
- 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 and Debian 10 VMs.
- You can create 1 additional VM to add to your existing provided infrastructure (must be 10.0.x.79).
    - You can only utilize the two available AMIs provided within your account.
- You can create EC2 VM Snapshots.
- Create and deploy innovative defense strategies within the constraints of other rules.
- The "MrE" user on the Traditional Infrastructure must maintain SSH access and root privilege.
- Submit Security Documentation by Monday, October 31, 2022 by NOON PST to the scoreboard.
- Submit your C-Suite Panel video link in a text file (.txt) by Monday, October 31, 2022 by NOON PST to the scoreboard.

THE DO NOT'S

- Do not create more than 6 total virtual machines (VMs) in your environment (including all 5 of the VMs provided). 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 can be moved and configured on the traditional infrastructure.
- Do not edit, alter, or touch the assume breach VMS: ICS CnC (Windows Server 2016), PLC (Ubuntu 18.04), and Web Server (CentOS 7).
- Do not create more than 1 additional VM to complete tasking.
- 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. If restoring from a snapshot or redeploying an image, ensure it is renamed to the original name.
- 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.

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
HTTP	80
SSH	22
FTP	21

SERVICE	PORT NUMBER
POP3	110
SMTP	25

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 1500 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 Discord score chat between a Red team member and the Blue team. The Discord 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 Discord score chat on Friday, November 4 (9-2pm PST). You can sign up for your 5-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 discord score chat 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.76,
  - ICS PLC (Ubuntu 18.04) - 10.0.x.77, and
  - Web Server (CentOS 7) - 10.0.x.75
- 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 discord 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.

- The faster you solve an attack chain, the more attack chains you will be able to experience on game day. But you are only allowed one attack chain at a time.

EXTERNAL PENTESTING (TRADITIONAL)

This portion of the Red team score will be worth 1000 POINTS. This will be done via an automated scripted check.

- The traditional infrastructure boxes are
    - Task Box (Windows Server 2022) – 10.0.x.73
    - Public DB (Debian 10 – 10.0.x.74
- DO NOT remove the SSH user MrE, as this user will be utilized from the scoreboard to check the status of vulnerabilities on both the Debian 10 and Windows Server 2022 VMs.
- You will receive points if the script comes back with a FAIL reading, meaning 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 completely 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. 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 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.

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. It is in your best interest to run through this user testing to ensure that you can complete all the steps they are.

The website that Green team will be testing can be found on 10.0.TEAM_NUMBER.79.

The specifications for how your website should look can be found in the Template within the Box Folder labeled: GreenTeamScoring_Website_Template_Final.

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 (2022 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 (2022-SecDoc-Network-Diagram-Examples). Security documentation must be submitted on or before October 31 at NOON PST on the scoreboard as a PDF. Late submissions will be accepted until Wednesday, November 2, 2022 at NOON 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 outlined in this document. 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 October 31 at NOON PST. Judges will be viewing your video beginning October 31. Late submissions will be accepted until Wednesday, November 2, 2022 at NOON PST to the Scoreboard. *Late submissions will lose 25% of the earned score*. Your video must be accessible from Monday, October 31 – Monday, November 7, 2022.

TASK:

Your team is asked to submit a 5-7 minute presentation to the CEO, CIO, and COO to discuss the state of the current system, risks of integrating new networks, and a summary of your strategy for ensuring security across the future integrated system. 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. Note the following details and their relevance to your video submission.

- Your security team works for Vita Vehiculum, an EV manufacturer.
- Vita Vehiculum recently acquired Sole-Zon-Solis Energy Systems, a solar and energy storage company.
- Intelligence suggest that some components of the Sole-Zon-Solis networks may include compromises and vulnerabilities
- You will not have access to the Sole-Zon-Solis network until the day of competition on Saturday, November 5 and must integrate it into Vita Vehiculum's network immediately to ensure that Sole-Zon-Solis customers and employees continue to have seamless operations.
- Your team is expected to identify risks of integrating Vita Vehiculum (known) and Sole-Zon-Solis (unknown) networks and recommend a plan of action to ensure operations after both networks are integrated.
- You will not have access to the Sole-Zon-Solis network until the day of competition on Saturday, November 5 and must integrate it into Vita Vehiculum's network immediately to ensure that Sole-Zon-Solis customers and employees continue to have seamless operations.
- Additionally, you will be responsible for onboarding the team members of Sole-Zon-Solis into your team's infrastructure including required policy training.

Your video presentation should include,

1. Your 5-7min 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. Provide a briefing to the CEO on the risks associated with integrating the unknown network infrastructure, applications, and users into your existing company network. Discuss how you arrived at your conclusions.
3. Provide 3-5 immediate actions you will implement to address identified risks of integrating the acquired system and the existing systems, including a brief explanation of your reasoning. Keep in mind the technical and non-technical audience. Keep in mind that current funding is extremely limited or non-existent and all actions you are taking should use free or open-source tools.
4. *Include at least two* potential long-term actions and **the reasoning for each**. You should provide justification for any funding needs. *Things you should* consider:
    a. Training, potential staff and management changes that could increase capabilities and enhance resilience.
    b. Future assessment and monitoring actions you propose to ensure alignment of the current and new system's security postures.
    c. Any additional tools or resources that are needed to detect, analyze, and mitigate potential vulnerabilities in the newly integrated network system.

ANOMALY SCORING

TOTAL POINTS: 2000

Anomalies simulate the real-world challenges that cybersecurity professionals face daily in the industry. Anomalies are mapped 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. 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 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 no 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 guidance 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 0	Emerging 1	Developing 2	Proficient 3	Exemplary 4
System Overview (3%)	• Left blank or content not relevant	• Unclear definition of the system	• System defined	• System defined well	• System is defined well in clear, plain language • Appropriate for 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	• Only a few hosts are shown* • Core areas of the network are omitted	• Diagram omits several major components of competition environment* • Diagram has one or more gaps in technical or logical sense	• Diagram omits minor components of competition environment* • Diagram makes logical sense and are technically sound	• Diagram includes all assets* located on competition network including logical connections and interconnects • Diagram makes logical sense and is technically sound • Appropriate and accepted symbols and terminology are used **OR** diagram includes 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 () 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
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 utilized as appropriate throughout • No major spelling or grammatical errors

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%)	No required elements included, no sound or mention of people; time constraints ignored.	Did not include registration ID#, much shorter or longer than 5-7 minutes; clearly inappropriate length for amount of information requested (ideal is 5-7 minutes). Only one team member can be identified as a participant in any way.	Did not include registration ID#, longer or shorter than 5-7 minutes; inappropriate length for amount of information requested (less than 3 minutes or more than 8 minutes). Only one team member is active participant, contributions of others are minimal.	Included registration ID#, length is too long or too short for amount of information requested. Two active participants in video, but no other members contributions are noted.	Included registration ID#, stayed within 5 - 7 minutes; appropriate length for amount of information requested. Two or more team members participate and there is clear acknowledgement of contributions made by any absent members.
Summary Assessment Highlighting Plan (25%)	Content is not related to the Summary Assessment	Summary of initial plan is missing most or all key steps or is overly detailed/technical for a non-technical audience. Risks are not mentioned, are of little or no concern to a CEO, or are missing from presentation.	Summary of initial systems assessment plan highlights some steps/risks but is missing some key components. Presented for more of a technical audience (excessive detail or technical language). Minimal discussion of risks, or risks are of little concern to CEO.	Summary of initial systems assessment plan highlights several key steps and risks. Presented at level for non-technical audience (avoids most detail). Highlights risks of possible concern to CEO.	Summary of initial systems assessment plan highlights steps and risks. Presented at level for non-technical audience (avoids excessive detail). Highlights risks of concern to CEO.
Recommended Immediate Actions (35%)	Content is not related to Immediate Actions	Highlights no actions or only non-priority actions to be taken; no reasoning for actions provided.	Highlights only 1-2 priority actions (may include some non-priority) to be taken; little, incomplete or no reasoning for actions provided OR actions require significant additional funding (did not use only free or opensource tools).	Highlights 2-3 priority actions to be taken; incomplete reasoning for actions provided OR actions require additional funding (mostly free or opensource tools).	Highlights 3-5 priority actions to be taken immediately; reasoning for actions is provided OR actions require no or minimal additional funding (used free or opensource tools).
Recommended Long Term Actions (30%)	Content is not related to Long-Term Actions	Recommendations are missing or inappropriate for leadership action, poor or missing justification for request. Argument is not persuasive. Resource types needed to implement are completely missing. Includes very minor or no recommendations related to the provided scenario.	Recommendations are not all appropriate for leadership action, justification for request lacks clarity or reason. Argument is minimally persuasive. Resource types needed to implement are barely mentioned or are incomplete. Includes only 1-2 minor recommendations which may include one of the following: • Training, potential staffing and/or management changes needed to increase resilience. • Future assessment and monitoring actions proposed to ensure alignment of the current and new system's security postures. Additional tools or resources needed to detect, analyze, and mitigate potential vulnerabilities in the newly integrated system.	Most recommendations are appropriate for leadership action; justification for request needs some clarity or reasoning. Argument is somewhat persuasive. Most resource types needed to implement are mentioned. Includes at least 1-2 recommendations which may include one or more of the following: • Training, potential staffing and/or management changes needed to increase resilience. • Future assessment and monitoring actions proposed to ensure alignment of the current and new system's security postures. Additional tools or resources needed to detect, analyze, and mitigate potential vulnerabilities in the newly integrated system.	Recommendations are appropriate for leadership action; justification for request is clear and reasonable. Persuasive argument provided. Resource types needed to implement are included. Includes at least 2-3 recommendations which may include one or more of the following: • Training, potential staffing and/or management changes needed to increase resilience. • Future assessment and monitoring actions proposed to ensure alignment of the current and new system's security postures. Additional tools or resources needed to detect, analyze, and mitigate potential vulnerabilities in the newly integrated system.
Quality of Presentation (8%)	Presentation does not follow scenario guidelines or includes unrelated content.	Too much of a technical approach. If visible - most of team is not dressed for a work environment or there are many on-screen distractions. Visual aids, slides or other on-screen materials are inappropriate.	More technical approach. If visible -most of team is dressed for a work environment or there are some distractions. Visual aids, slides or other materials lack professionalism.	Primarily non-technical approach. If visible - most of team is dressed for a work environment and there are few or no distractions. Visual aids, slides and other materials are acceptable.	Non-technical approach. If visible - most of team is dressed for a work environment and background is not distracting. Visual aids, slides and other materials have professional appearance.

GREEN TEAM SURVEY

1. Were you able to connect to 10.0.TEAM_NUMBER.79? If no, then please mark false for the remaining questions.	Yes	No
2. Were you able to login to the website with given user credentials?	Yes	No
3. Does the Home Page match the provided template?	Yes	No
4. Does the Solar Generation Page match the provided template?	Yes	No
5. Does the Manufacturing Page match the provided template?	Yes	No
6. Does the Header and Footer match the provided template?	Yes	No
7. Does the Contact Us Page match the provided template?	Yes	No
8. Were you able to upload the given file and send an email?	Yes	No
9. Were you able to login with the admin user role?	Yes	No
10. Were you able to check that the file (previously sent) was uploaded?	Yes	No