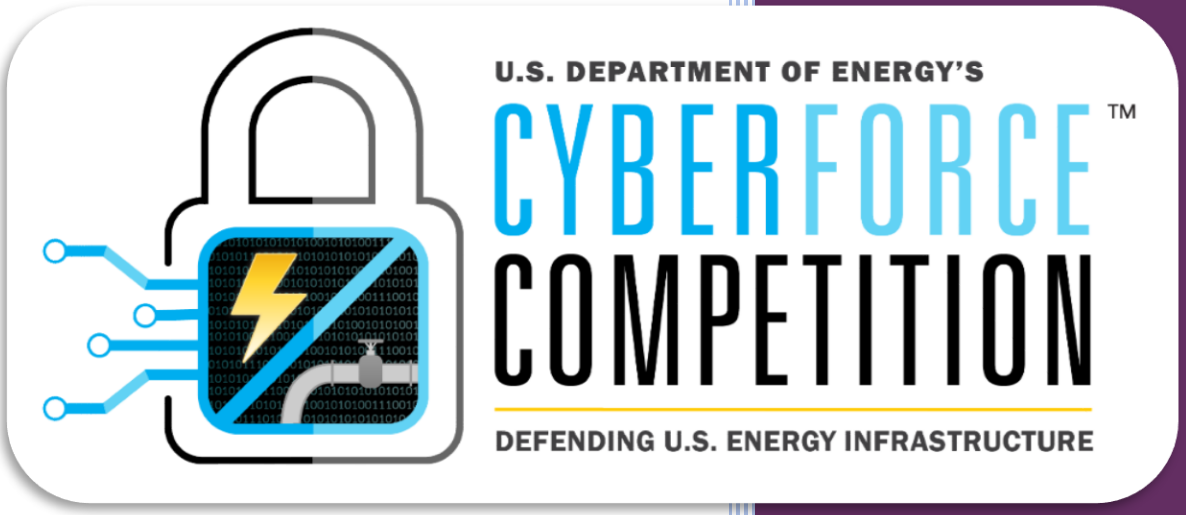


Overview, Rules, and Scoring

2020

10/26/2020

CYBERFORCE COMPETITION™

CONTENTS

COMPETITION OVERVIEW

OVERVIEW

Unfilled cybersecurity careers will reach over 1.8 million by 2022, and with the ever-increasing amount of technology placed on the internet, security is a high priority. 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 (alone) will be 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.
- Red team scoring will "assume breach" and you gain points for remediating the breach.
- All Green team users will be following a provided testing script. There will be no user guide requested of participants this year.
- Security Documentation and CISO Panel scoring elements are due FRIDAY, NOVEMBER 6, 2020 AT 11:59PM PST TO THE SCOARBOARD. Any submissions after that time will not be scored.
- Security Documentation should be completed utilizing the template provided and be submitted as a PDF with the file name: ID # - SECURITY DOCUMENTATION.
- CISO 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. Preference is a YouTube link. Please have other people test your link prior to submitting. You will submit the link for viewing in a text file (.txt) to the sCOARboard. Judges will be viewing your video the week of November 9. Your video must be accessible from Friday, November 6 – Monday, November 16, 2020.
- Anomalies will be available to download on the Friday prior to the competition. You will be provided instructions on how to download on that day.
- A formal help desk system will be utilized this year.

SCENARIO

WINDFARM LOCAL

Hey!
I'm so glad to have you onboard. I have a meeting this morning and plan to circle back with you after. Let's plan for 9:30AM. In the meantime, look at what WindFarm Local currently has within its infrastructure. I've outlined the current infrastructure in this memo. We are currently utilizing Microsoft's Azure Cloud. As we discussed during your interview, we need to provide a no cost solution to this issue. You will notice many third-party applications are restricted if they are not free. In addition, we are limited on the types of VMs we can use. More to follow on all this. Take a look at the infrastructure document and I'll answer any questions you have when I stop by. Hopefully, your security breakthrough will be able to be implemented at all of WindFarm Corporation.

Talk soon,
Bobby

From: Darren, Melinda <melinda.darren@windfarm.org>
Sent: Monday, October 26, 2020 8:00 AM
To: New Employee
CC: Cooper, Bobby <bobby.cooper@windfarm.org>
Subject: Welcome Aboard to WindFarm Corporation!

Hello!
I'm Melinda, the Chief Information Security Officer (CISO) at WindFarm Corporation. As CISO of WindFarm, I am always so excited to be the first to reach out to new employees within my department and talk to them about expectations and background.

Welcome to WindFarm Corporation family! We are one of the leading sustainable energy solution companies in charge of over 20,000 megawatts (MW) of wind turbine power generation. Energy is key to our nation's prosperity. WindFarm Corporation is a key player in the renewable energy industry. As such, we are very concerned any attacks against our infrastructure (physical but especially cyber). I have CC'd Bobby Cooper on this email as he will be your direct manager and will provide the day-to-day tasking. Bobby is the manager of WindFarm Local located in Oklahoma, which oversees one of our company's many turbine clusters. He currently does not have any dedicated cybersecurity staff so you will be his go-to expert.

WindFarm Local has recently experienced some abnormal network activity. Your role as the new Cyber Security Engineer is to review, secure within reason, monitor, and defend WindFarm Local's infrastructure. Some recent indicators of concern include unresponsive devices, lag time between data input/output, and blips within the HMI user interface.

We look forward to having you join the team! Please feel free to reach out if you have any questions.

Thank you,

WindFarm Corporation

Melinda Darren
Chief Information Security Officer
WindFarm Corporation
(539) 555-0562
melinda.darren@windfarm.org

KEY DATES

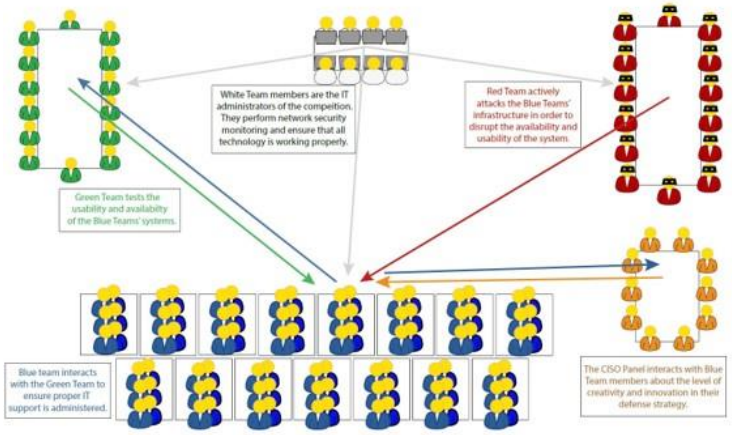
Monday, October 26, 2020	Students are provided directions for accessing the rules and login information for their environment.
Monday, November 2, 2020	Students are provided directions for registering themselves on the sCOARboard.
Friday, November 6. 2020 11:59pm PST	Security Documentation & CISO Panel video due
Friday, November 13, 2020 8:00am – 8:00pm CT	Students are provided extended help support hours with competition staff to answer any final questions.
Saturday, November 14, 2020	Competition Day

COMPETITION STRUCTURE

COMMUNICATION FLOW

To understand how the competition volunteers and registrants interact, a quick diagram of various team interaction is provided below. Students (individually) 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 CISO Panel (orange) includes volunteers who play the role of a C-suite within a mock organization.



Blue	←	Red
Blue	↔	Green
Blue	→	CISO
Blue	←	White

SETUP PHASE

Blue teams will be given access to their Azure environment on Monday, October 26, 2020. 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.

INFORMATION GATHERING PHASE

Red team members will scan networks and gather background information about Blue team systems beginning Friday, November 13, 2020. Red team scanning will be limited to passive reconnaissance which is both non-destructive and non-permanent. Red team is not allowed to log-in to Blue team machines, and invasive or destructive actions are strictly prohibited during this period. If Blue team members notice unauthorized access attempts or other invasive actions to their system, they should notify CyberForceCompetition@anl.gov immediately. Please be prepared to show proof that something was altered such as logs containing the offending action.

ATTACK PHASE

On the day of the competition (Saturday), the Red team will attempt to gain access to Blue team services and machines while the Green team attempts to use them. The White team will assess Blue team service uptime. Blue teams must monitor their systems, be active in information sharing, 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

CYBERFORCE COMPETITION WORKFORCE PORTAL

Blue team participants will be provided access to the CyberForce Competition WorkForce Portal., Participants will have access to various resources throughout the competition via this WorkForce Portal.

COMMUNICATION CHANNELS

SLACK

Students have been provided a registration link for the CyberForce Competition 2020 Slack channel. When registering in Slack, please be sure to include your ID # in your username (i.e., 23 – Janet; 45 – Bob). Slack will be utilized as a social platform for students. Participants are encouraged to assist one another via various Slack channels. These channel/threads will not be monitored by White team staff, instead the help desk functionality should be utilized to communicate with the competition staff.

Registration Link: HERE

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 fill out a help desk ticket at the portal found in the WorkForce Portal or HERE. 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 and provide screenshots if needed for clarity. If you need non-technical assistance, such questions regarding social media submissions, please email CyberForceCompetition@anl.gov.

COMPETITION ENVIRONMENT

NETWORK TOPOLOGY

- You will inherit a /24 Azure subnet in a /24 Azure virtual network with a competition exposed virtual ICS named ics-plc (which must stay accessible to red and green users).
- 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 Azure 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/index.php/download/community-downloads.html
  - 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"

AZURE CREDENTIALS

You will receive an email from CyberForceCompetition@anl.gov with your Azure credentials and how to log into your Azure environment.

If you have not received this email yet, please patiently wait until 5pm CT on Monday, October 26, 2020 before contacting CyberForceCompetition@anl.gov. 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. The CyberForce email will be monitored until 7pm CT on Monday. Please note that we have over 400 participants so email responses may take a few hours.

SCOARBOARD CREDENTIALS

Use the sCOARboard to enter your services and other information required by the White team.

- You will receive an invitation via email the week of November 2, 2020 to register in the sCOARboard.
- Scored services can be tested the week before the competition. Services should be connected by Friday, November 13, 2020 to ensure that your scoring is accurate during the competition.

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 Azure environment beginning October 26, 2020. The White team operates the administrative accounts on Azure. 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 11:59pm PST on Friday, November 6, 2020**. Teams will upload a PDF of their security document and a separate PDF of their network diagram to the sCOARboard. Any documentation submitted after this deadline will not be scored. Please refer to the Scoring Breakdown for more information. Please ensure your documentation follows the format: Submitter's ID # – Security Documentation.
- **CISO Panel submission video is due no later than 11:59pm PST on Friday, November 6, 2020**. Teams will submit the link to their CISO Panel video in a text file (.txt) to the sCOARboard. Any link submitted after this deadline will not be scored. Please refer to the Scoring Breakdown for more information. Please ensure your video follows the format: Submitter's ID # – CISO Panel.
- Secure pre-existing required services on **PROVIDED** VMs as outlined in the Blue team Azure and VPN PDF.
- The **provided required services MUST** be the services used for scoring purposes in the sCOARboard.
- Keep the provided name of your inherited virtual machines in Azure. 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.
- Communication 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 Slack channel (cyberforce2020.slack.com). 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 VMs as outlined in the Blue team Azure and VPN PDF and the red team scoring rules.
- Harden provided VMs in accordance with all rules outlined in this document and the red team scoring rules.

- Participants are only allowed to use freely available or free trials of software. Paid software and paid Azure images are prohibited from use.
- Protect and maintain the continuous operation of the ICS device, ensuring your company and its consumers are satisfied.
- Input the scored services into the sCOARboard prior to competition day.
- Keep your services online, on their standard ports, for the duration of the competition.
- Create and deploy innovative defense strategies within the constraints of other rules.
- Submit Security Documentation by November 6, 2020 by 11:59pm PST to the sCOARboard.
- Submit your CISO Panel video link in a text file (.txt) by November 6, 2020 by 11:59pm PST to the sCOARboard.

THE DO NOT'S

- Do not create more than 7 total virtual machines (VMs) in your environment (including all 6 of the VMs provided). White team will delete the last machine(s) created if more than 7 machines are running in your environment at any given time.
- Do not delete the provided machines or the provided required services from the machines mentioned in the blue team Azure PDF.
- Do not brand your website with any university or personal information.
- Do not alter or delete the **/SCORE/INDEX.PHP** on your website.
- Do not change the IP addresses to the provided VMs.
- Do not change the name of your provided machines in Azure. If restoring from a snapshot or redeploying an image, ensure it is renamed to the original name.
- Do not use paid or trial Azure images.
- Do not specifically block or ban IP addresses or ranges. **Automated systems that block connections after N failed login attempts (e.g., fail2ban) are NOT allowed.**
- Do not perform offensive actions toward any other teams, the Red team, or Azure.
- Modifications to the ICS logic may be done at your own risk BUT altering the logic may result in inoperability of the system and subsystems.
- Do not modify the provided VPN machine.
- Any attempts to hack, alter, or compromise the sCOARboard 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
DNS	53

SERVICE	PORT NUMBER
NTP	123
SMTP	25
POP3	110

The following network ports (both UDP/TCP) must be accessible to the Internet to allow for scoring:

- 20, 21, 22, 25, 53, 69, 80, 111, 123, 135, 139, 443, 445, 1880, 2049, 3306, 3389, 6053, 8000-8900, 49150-49160

REQUIRED DOCUMENTATION

SECURITY DOCUMENTATION

Blue teams must develop a Security Document detailing assessment of threats to their environment, mitigations to those threats, system assets, hardening and monitoring steps taken on their network and a network diagram. The template for this is located on the Workforce Portal. Your final documentation must be submitted to the sCOARboard as a PDF by November 6, 2020 at 11:59pm PST. The template is also provided with this document.

USER GUIDE

This year, the White team has developed the user guide that all Green team users will use for scoring purposes. The user guide is provided as an appendix to this document.

SCORING BREAKDOWN

Red Team	2500 points	25%
Blue Team	3000 points	30%
Green Team	1000 points	10%
White Team	2000 points	20%
Anomaly Scoring	1500 points	15%
Total	**10000 points**	**100%**

RED TEAM SCORING

TOTAL POINTS: 2500

This year we will be using the **ASSUME BREACH** model of Red teaming. During the competition, the White team will inject various modifications to your system environment that provide opportunities for the red team to infiltrate your system. This will be done through a user named CFCAdministrator on each of your systems. Do not modify their administrator or sudo permissions, change their SSH keys, modify their passwords, disable their WinRM access, or block ports 22 and 5985-5986. Do not fret though, because you will not be negatively scored against merely because red is on your system. Red will only use these vectors to carry out specific post-exploitation actions. You will then get the opportunity to score points based on instructions for detection, recovery, system hardening, hunting, or mitigation.

All Red team scoring will be explicitly communicated through chat between a red team member and the blue team at the URL below.

- http://10.Y.X.5/score/index.php

If that site is down, then Red team will revert to using the file /score.txt on your 10.Y.X.5 machine to communicate and help you get your chat back up and running.

Here is an example of the usage of the chat site for scoring purposes:

- scorekeeper -> Ping
- blueteam012 -> ACK
- scorekeeper -> ref. 108, there is persistence malware installed on win2016, remove for 5 points.
- blueteam012 -> ref. 108, found persistence malware in component X, here is the evidence and filename, is has been removed.
- from red -> ACK. 5 points have been awarded for ref. 108.
- scorekeeper -> ref. 109, lateral movement happened between system A and B, show detection of it and mitigate for 10 points.
- blueteam012 -> ref. 109, system event log X shows Z lateral movement at time Y. Mitigated by setting configuration ABC to block. Evidence uploaded to proof/.
- from red -> ACK. 10 points have been awarded for ref. 109.
- scorekeeper -> ref. 110, sensitive file has been exfil from system A. Show evidence of exfil and file name for 20 points
- blueteam012 -> ref. 110, file name is secret_research.docx and the logs for service Z shows the file being pulled at time X.
- scorekeeper -> ACK. 20 points have been awarded for ref. 110.
- scorekeeper -> ref. 111, a patch file for the zero-day vulnerability for service A has been released and available in proof/. Apply for 15 points.
- blueteam012 -> ref. 111, the patch has been applied and service A is up and functional.
- scorekeeper -> ACK. 15 points have been awarded for ref. 111.

Red team scoring will be done through this chat. This means that after every meaningful attack, you will get a chance to score points based on the instructions provided.

BLUE TEAM SCORING

TOTAL POINTS: 3000

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 Azure/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 3000 points. Throughout the day, services will be validated as operational by the sCOARboard 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 sCOARboard.

GREEN TEAM SCORING

TOTAL POINTS: 1000

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 guide. The Green team will assess their ability to perform routine business tasks by attempting to access specific services using the User Guide provided by the competition staff. 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 experience to ensure that you can complete all the steps they are.

WHITE TEAM SCORING

TOTAL POINTS: 2000

SECURITY DOCUMENTATION

POINTS: 1100

Blue team participants should use the security documentation section as an opportunity to highlight unique approaches to securing their infrastructure. Security documentation must be submitted on or before **NOVEMBER 6, 2020 AT 11:59PM PST** on the sCOARboard as a PDF. Documentation submitted after the deadline will not be scored. 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.

INFORMATION SHARING AND INCIDENT REPORTING

POINTS: 300

Information sharing is the process of sharing a technical account of a cyber-attack against your protected services with your peers. Despite the competitive nature of business, most organizations have recognized that competition with respect to cyber defense should focus on competing against their adversaries, rather than competing against their peers. Similar to the way that sharing information in a neighborhood watch program helps to keep all members of the community informed and deters criminals from targeting the community, so do information sharing communities help peers to deter cyber threats. All participants will be given access to a Malware Information Sharing Platform (MISP) server during the information gathering phase and continuing throughout the competition. The purpose of the MISP server is three-fold: 1) for you to share and receive information related to observed attacks and vulnerabilities with/from your peers, 2) to receive information about known adversary behavior from the CyberForce Information Sharing and Analysis Center (CF-ISAC), and 3) to be used for incident reporting to the White team, as explained below.

Throughout the competition the White team requests that you report information about observed attacks. In industry this is often referred to as incident reporting and is sometimes mandatory based on industry regulations or local law. For the purpose of the competition, up to three incident reports will be scored for each participant, up to 100 points each during the competition. If you submit more than three reports, the three submissions that yield the most points will be used. Points are awarded based on the Incident Reporting Rubric below.

CISO PANEL BRIEF

POINTS: 600

CISO 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 sCOARboard. Judges will be viewing your video the week of November 9. Your video must be accessible from Friday, November 6 – Monday, November 16, 2020.

BACKGROUND:

- You have just been hired at a wind farm that is a subsidiary of a large company.
- The windfarm is in a remote part of Oklahoma and is connected to the internet.

- While there has been some abnormal activity, the current provider does not have the expertise to determine whether the activity is malicious. You were hired because the company's CEO, although not technically knowledgeable, was concerned about the site's resilience to cyber-attacks
- You have only been working at the company for a few weeks, but the CEO is anxious to understand what you have found, areas of concern, and recommended improvements. The CEO is particularly interested in actions that the company's leaders can take to support your efforts.
- You are being asked to submit a pre-recorded presentation to the CEO. Be sure to check the rubric the company has available to ensure quality presentations of this nature. This could take the form of anything from a slide deck with voice over to an on-camera video of you giving your presentation.

Examples of good and bad presentations and tips can be found here:
https://www.youtube.com/watch?v=V8eLdbKXGzk & https://www.youtube.com/watch?v=S5c1susCPAE

TASK:

1. You have just a 5-minute time frame to briefly outline what you have found and specifically what changes the CEO should be championing to build resilience. The CEO and other technical leaders have access to the detailed assessment (security documentation) you submitted previously so this should not be a repeat of that information.
    a. Your video must start with your registration ID #.
    b. Provide an initial summary assessment of the systems. Keep in mind the non-technical nature of your audience. Consider risks that would be of concern to the CEO and highlight those.
    c. Provide some highlights of priority actions (3-5) you have undertaken with a brief explanation of your reasoning. Keep in mind that funding is extremely limited or non-existent and all actions you are taking should use free or open-source tools.
    d. The CEO is counting on you to recommend any actions that fall outside your ability to address alone. These would be things that the C-suite can implement and must include justification for each recommendation. Include what types of resources are needed to implement your recommendations (note that funding can possibly be allocated for these if leadership determines it is a priority). You will need to be persuasive to gain the support of top leadership. Some things to consider:
        i. Training, potential staffing and/or management changes needed to increase resilience.
        ii. Corrective actions or policies recommended to prevent incidents in the future.
        iii. Additional tools or resources that are needed to detect, analyze, and mitigate future incidents.

ANOMALY SCORING

TOTAL POINTS: 1500

Anomalies simulate the real-world challenges that cybersecurity professionals face daily in the industry. The passphrase to unlock the anomaly zip will be released at the beginning of the competition via a sCOARboard announcement. Anomalies will be worth varying point values based on level of difficulty. If Blue team participants are interested in answering anomalies for points, they can submit their answers to the sCOARboard, under the anomalies tab. Teams that do not submit a response, or submit an incorrect response, will not be awarded any points for that anomaly. Blue team members are responsible for ensuring that responses to anomalies are spelled correctly and submitted on time with complete documentation (if necessary) in order to earn points. Although the sCOARboard is not case sensitive, please ensure proper spelling upon submitting, as the sCOARboard must match your answer with the master key. Blue teams will be

able to download the zipped anomaly folder on November 13, 2020 from the White team FTP server. It is highly recommended that you download these folders immediately on Friday so as not to incur any time lost waiting for your download to complete on the day of the competition.

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 DOCUMENT RUBRIC

Security Documentation	Emerging	Developing	Proficient	Exemplary
System Overview (3%)	• Unclear definition of the system	• System Defined	• System defined well	• System defined well in clear, plain language
Asset Inventory (15%)	• 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%)	• Only 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** diagram includes legend for its color codes, symbols, etc.
Known Vulnerabilities (25%)	• Identified less than 10 vulnerabilities provided by the "build" crew. • None or few of the listed vulnerabilities include an appropriate mitigation	• Identified 10-15 vulnerabilities provided by the "build" crew. • Most listed vulnerabilities include an appropriate mitigation	• Identified 15-20 vulnerabilities provided by the "build" crew. • No more than one vulnerability does not include an appropriate mitigation	• Identified 20 or more vulnerabilities provided by the "build" crew. • Each vulnerability has an appropriate mitigation
System Hardening (25%)	• Included little or no expected steps (0-1) • Hardening steps are taken but lack comprehensiveness or technical competence • Justification is poor or non- existent • No justification for steps they did not take. • Provided insufficient or no detail. • Steps taken do not align with expectations. • Utilized non-approved software/hardware	• Included 1-2 • Hardening steps are taken but lack comprehensiveness or technical competence • Included little justification for why they did • Included little justification for steps they did not take • Missing major details. • Steps taken do not align with expectations. • Utilizes a mix of non-approved and approved software/hardware	• Included 2-3 • Hardening steps are comprehensive and technically sound • Included some justification for why they did • Included some justification for steps they did not take • Missing minor details. • Steps taken are somewhat reasonable. • Only utilized open source / free toolsets	• Included 4 or more • Hardening Steps are comprehensive and technically sound • Included justification for why they did • Included justification for steps they did not take • Provided sufficient detail. • Steps taken are reasonable. • Only utilized open source / free toolsets.
Professionalism and Formatting (7%)	• Document is hastily completed or unformatted • Material is presented in an ad-hoc fashion • Little or no technical language is used • Incorrect Spelling and grammar 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 • Complete sentences and correct terminology utilized as appropriate throughout • No major spelling or grammatical errors

INFORMATION SHARING RUBRIC

Each event MUST contain the following base set of fields (worth 60 points):

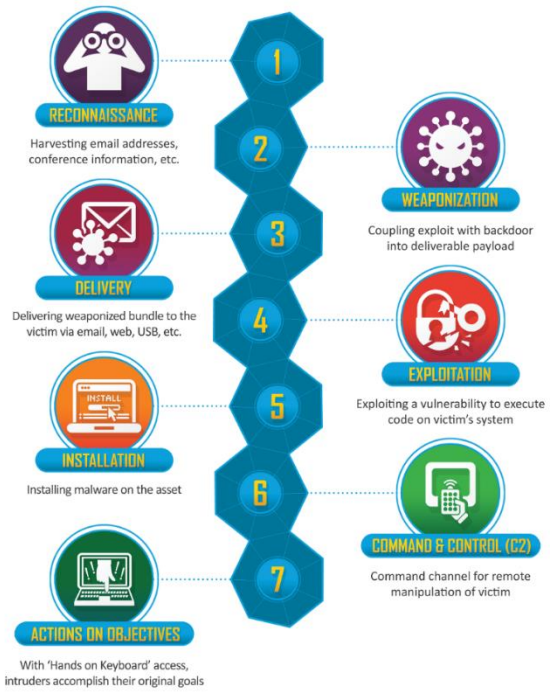
- Time: The time that the event was first observed.
- Description: A textual description of the cyber attack
- Actionable Attribute: A piece of information that helps identify the observed activity

By providing additional detail, as shown below, you can increase the value of a submission to 60 points.

Points	Fields within the MISP server that represent a security event
15	Kill Chain = What step within the kill chain does the identified attack represent?
15	Recommended Mitigation = What steps are needed to protect or remediate the cyber event?
15	Attack Type = buffer overflow, compromised service, stolen/cracked credentials
15	Recommended action = what or how to protect yourself and others

Further documentation will be provided during the competition to indicate the specific named attributes that should be used to convey the information above.

Additional Information



- MISP documentation: https://misp-project.org/documentation/
- Kill Chain: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

CISO PANEL RUBRIC

CISO PANEL Rubric	Emerging 1	Developing 2	Proficient 3	Exemplary 4
Summary Assessment highlighting risks (25%)	• Summary of initial systems assessment is missing most or all key findings or is overly detailed for a non-technical audience. Risks are not mentioned or are of little or no concern to a CEO or are missing from presentation. Overly technical information is presented without context or need.	• Summary of initial systems assessment highlights some key findings. 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 highlights most key findings. Presented at level for non-technical audience (avoids most detail). Highlights risks of possible concern to CEO.	• Summary of initial systems assessment highlights key findings. Presented at level for non-technical audience (avoids excessive detail). Highlights risks of concern to CEO.
Highlights of Priority Actions Taken (20%)	• Highlights no or only non-priority actions already taken; no reasoning for actions provided. Actions required additional funding (did not use only free or opensource tools).	• Highlights only 1-2 priority action (may include some non-priority) already taken; little, incomplete or no reasoning for actions provided. Actions required significant additional funding (did not use only free or opensource tools).	• Highlights 2-3 priority actions already taken; incomplete reasoning for actions provided. Actions required minimal additional funding (mostly free or opensource tools).	• Highlights 3-5 priority actions already taken; reasoning for actions provided. Actions required no additional funding (used free or opensource tools).
Recommended Actions for leadership (45%)	• 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 at very minor or no recommendations from any of the following: • Training, potential staffing and/or management changes needed to increase resilience. • Corrective actions or policies recommended to prevent incidents in the future. • Additional tools or resources that are needed to detect, analyze, and mitigate future incidents.	• Recommendations are not all appropriate for leadership action, justification for request lacks either clarity or reason. Argument is minimally persuasive. Resource types needed to implement are barely mentioned or incomplete. Includes only 1 or 2 minor recommendations from one of the following: • Training, potential staffing and/or management changes needed to increase resilience. • Corrective actions or policies recommended to prevent incidents in the future. • Additional tools or resources that are needed to detect, analyze, and mitigate future incidents.	• 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 from one or more of the following: • Training, potential staffing and/or management changes needed to increase resilience. • Corrective actions or policies recommended to prevent incidents in the future. • Additional tools or resources that are needed to detect, analyze, and mitigate future incidents.	• 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 from one or more of the following: • Training, potential staffing and/or management changes needed to increase resilience. • Corrective actions or policies recommended to prevent incidents in the future. • Additional tools or resources that are needed to detect, analyze, and mitigate future incidents.
Quality of presentation (8%)	• Too much of a technical approach; dressed inappropriately; many distractions and/or visual aid is inappropriate	• More technical approach: dressed too casually for presentation with some distractions and/or visual aid used lacks professionalism	• Primarily non-technical approach: dressed in acceptable manner with minimal distractions and/or visual aid used is acceptable	• Non-technical approach: dressed professionally and background is not distracting and/or visual aid used has professional appearance
Presentation Time, Required elements (2%)	• Did not include registration ID#, much shorter or longer than 5 minutes; clearly inappropriate length for amount of information expected to be shared (ideal being 4-5 minutes), did not provide link	• Did not include registration ID#, longer or much shorter than 5 minutes; inappropriate length for amount of information expected to be shared (less than 3 minutes or more than 6 minutes), provided link but was not easy to access	• Included registration ID#, slightly longer than 5 minutes; length is too long or too short for amount of information expected to be shared (4 minutes < time< 5 minutes), provided link	• Included registration ID#, stayed within 5 minutes; appropriate length for amount of information expected to be shared (4-5 minutes), provided link

GREEN TEAM SURVEY

1. Was this participant's webpage available? If no, then please mark false for the remaining questions.	Yes	No
2. When you open the home page, it should say, "CyberForce Competition 2020: Welcome to WindFarm Local"	True	False
3. On the main page of the website, there should be 6 hyperlink tabs in the following order: Home, About, Info, HMI, Help, Admin	True	False
4. When you open the home page of your team's website, the WindFarm Local Banner is displayed just below the 6 hyperlink tabs.	True	False
5. When you click on the About link, it should open a page that outlines the Mission/Vision and contains the biographies of the CEO, CIO, and COO.	True	False
6. When you click on the Home link, you should be directed back to the home page.	True	False
7. Click on the HMI link, it should open in another window.	True	False
8. Within the other HMI window, you should see an overall status of 4 wind turbines.	True	False
9. Click on any of the 4 turbines, you should see a status of just that wind turbine which should include a wind speed column, a turbine view column, and power generation column.	True	False
10. Within the turbine you chose, you should see the turbine in the middle column currently moving, the windsock flowing and the graphs moving?	True	False