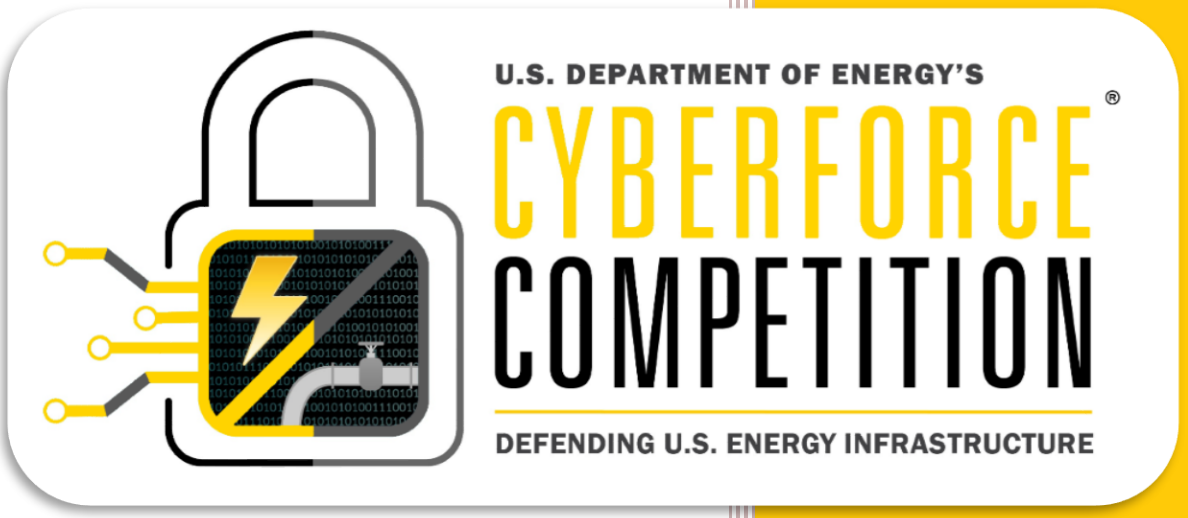


Overview, Rules, and Scoring

2021

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

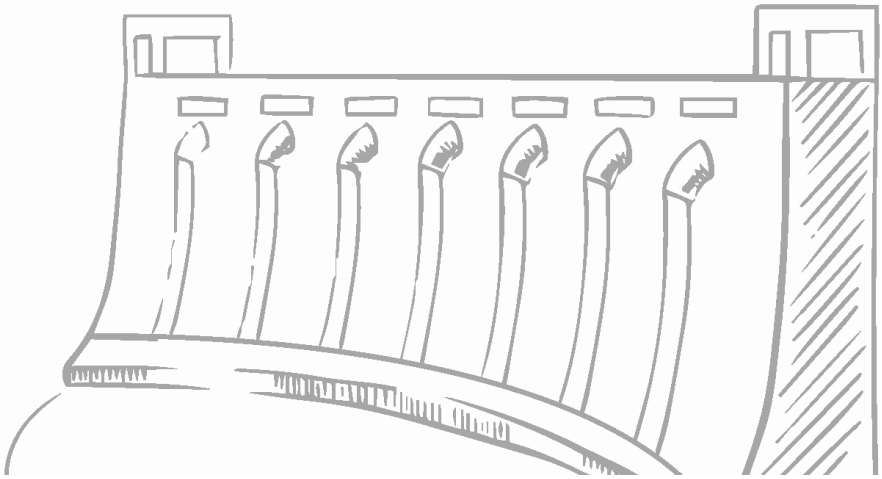
- For the purposes of competition, you will be the Blue team.
- Overall scoring breakdown can be found later in this document, the breakdown has been changed compared to prior competitions. Please take a moment to review this document thoroughly.
- Red team scoring will "assume breach" and you gain points 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 C-Suite Panel scoring elements are due TUESDAY, NOVEMBER 9, 2021 AT 11:59PM PST TO THE SCOARBOARD. Late submissions will be accepted until Thursday, November 11, 2021 at 11:59PM PST to the SCOARboard. *Late submissions will lose 25% of the earned score*.
- Security Documentation should be completed utilizing the template provided and be submitted as a PDF with the file name: ID # - SECURITY DOCUMENTATION.
- 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. 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 beginning November 9. *Your video must be accessible from Tuesday, November 9 – Tuesday, November 16, 2021.*
- Anomalies will be available to download on the Friday, November 12, 2021. You will be provided instructions on how to download via Discord.
- A formal help desk system will be utilized this year.

CyberForce Competition - Educational Purposes Only

INNOVO ELECTRIC

Innovo Electric, the Hydropower Energy of the South, has been a vital asset for local communities around Kuma Lake and Dam. Innovo recently acquired Moti, a small weather analysis company dedicated to providing prompt and accurate data reports to the local area. Moti is part of a large research coalition that utilizes a large datacenter to better compute and analyze the energy generation output throughout the United States. Innovo has made a promise to continue this research and provide valuable results.

Innovo is currently under a lot of pressure to ensure that the Kuma Lake and Dam facility is running efficiently and that the complex is meeting a high threshold of both physical and cyber security standards. To help with this objective, an external team has been brought into the facility to test the security posture and provide a full report diagnostic of their findings. There were more than the desired amounts of findings against our operations system. Your team's task moving forward is to better harden and secure Innovo and Moti the best you can from potential future issues.



KEY DATES

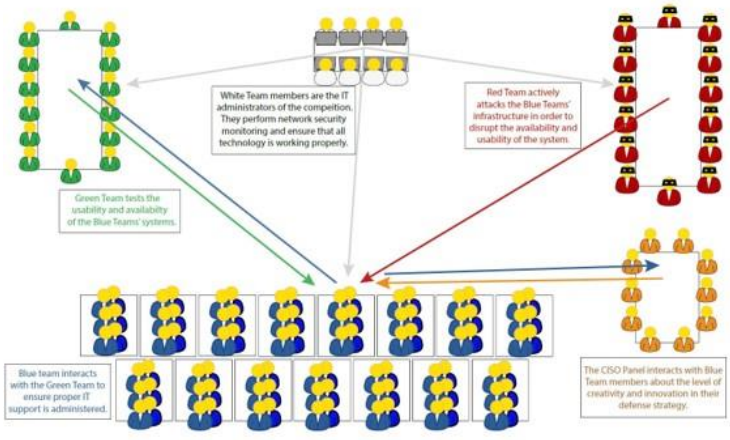
Monday, October 25, 2021	Students are provided directions for accessing the rules and login information for their environment. Discord invitation is provided.
Monday, November 1, 2021	Students are provided directions for registering themselves on the sCOARboard.
Tuesday, November 9, 2021 11:59pm PST	C-Suite Panel video due
Tuesday, November 9, 2021 11:59pm PST	Security Documentation due
Friday, November 12, 2021 8:00am – 8:00pm CT	Students are provided extended help support hours with competition staff to answer any final questions. Red team and Blue team mandatory check in.
Saturday, November 13, 2021	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 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.



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

SETUP PHASE

Blue teams will be given access to their Azure environment on Monday, October 25, 2021. 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 12, 2021. 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 CyberForceSupport@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 WORKFORCE PORTAL

Blue team participants will be provided access to the CyberForce Workforce Portal: CASTLE. Participants will have access to various resources throughout the competition via CASTLE. An email will go out once this portal is accessible to all.

COMMUNICATION CHANNELS

DISCORD

Students have been provided a registration link for the CyberForce Competition 2021 Discord Server. When registering in Discord, please be sure to include your Team # in your username (i.e., T23 – Janet; T45 – Bob). Discord will be utilized as a social platform for students. Participants are encouraged to assist one another via various Discord 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 send in a help desk ticket by sending an email to CyberForceSupport@anl.gov. 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/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"

AZURE CREDENTIALS

You will receive an email from atheel@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 25, 2021 before contacting CyberForceSupport@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 800 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 1, 2021 to register in the sCOARboard.
- Scored services can be tested the week before the competition. Services should be connected by Friday, November 12, 2021 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. A BACKUP GUIDE IS PROVIDED, BE SURE TO FOLLOW THESE INSTRUCTIONS.

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 25, 2021. 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 Tuesday, November 9, 2021**. Teams will upload a PDF of their security document and a separate PDF of their network diagram to the sCOARboard. Late submissions will be accepted until Thursday, November 11, 2021 at 11:59PM PST to the SCOARboard. *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 ID # – Security Documentation.
- **C-Suite Panel submission video is due no later than 11:59pm PST on Tuesday, November 9, 2021**. Teams will submit the link to their C-Suite Panel video in a text file (.txt) to the sCOARboard. Late submissions will be accepted until Thursday, November 11, 2021 at 11:59PM PST to the SCOARboard. *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 ID # – CSuite 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.
- Communications with White team members is 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 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.
- 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 Tuesday, November 9, 2021 by 11:59pm PST to the sCOARboard.
- Submit your C-Suite Panel video link in a text file (.txt) by Tuesday, November 9, 2021 by 11:59pm PST to the sCOARboard.

THE DO NOT'S

- Do not create more than 9 total virtual machines (VMs) in your environment (including all 7 of the VMs provided). White team will delete the last machine(s) created if more than 9 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 and VPN PDF.
- Do not modify **scorecheck01**, **scorecheck02**, and **greenteam02:** administrator or sudo permissions, change their SSH keys, modify their passwords, disable their WinRM access.
- Do not reset the Win2016 RDP administrator account.
- Do not block ports 22 and 5985-5986.
- 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 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 Blue 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:

- 22 & 5985-5986

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. A template has been provided and must be utilized. Your final documentation must be submitted to the sCOARboard as a PDF by November 9, 2021 at 11:59pm PST.

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

All 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 12 (12-8pm CT). You can sign up for your 15-minute slot HERE. NOTE: there are only limited slots per 15-minutes, so be mindful to register your team. 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. A list of open ports will be provided then and the scorekeeper will help you to check that your environment is ready for the competition. *You will be invited to this Discord just prior to your Friday, November 12 check-in.*

ASSUME BREACH

This year we will be using the **ASSUME BREACH** model of Red teaming. This will be worth 2000 POINTS. 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 the following accounts on each of your systems: **scorecheck01**, **scorecheck02**, and **greenteam02**. 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.

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. Besides the real time injections for all VMs, your Windows2016 VM is completely dedicated for assume breach. It highly recommended that you do not modify this VM, otherwise you'll lose opportunities to score points.

EXTERNAL PENTESTING

This portion of the Red team score will be worth 500 POINTS. This will be communicated through the score chat with the prefix of "PT", which stands for pentest.

The pentesters will not be given any info about these VMs for the first 3 hours of the competition. Scoring is not based on the pentester's success but based on the ability of the defenders to understand the activity and to successfully minimize the exposed risk. Points will be given for defensive measures that are realistic and would work in a real-world environment. No points will be given for unrealistic defenses that are based on the artificial constraints of the game environment (e.g., killing all new network connections - doing so in the real world would cause your hydro plant to fail). IT'S IMPORTANT TO CONSIDER HOW YOUR DEFENSIVE ACTIONS WILL AFFECT THE CRITICAL OPERATIONS OF YOUR SYSTEMS.

The pentester will go at a speed appropriate for the Blue team and will not overwhelm them. This will give the Blue team time to think through their situation and implement a good solution for their vulnerabilities instead of a hasty one. These activities will be communicated in the score chat for point assignments. After the 3rd hour, the pentester will be given information about vulnerabilities/exploits that they can gradually use against these VMs. Through a control mechanism to the VMs, additional changes will be added to the VMs. This will give the pentester opportunities to launch more attacks against new functionality and opportunities for Blue team to score points base on their defensive actions.

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 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.8:3000. You MUST keep your website on port 3000 for the Green team to be able to accurately score.

WHITE TEAM SCORING

TOTAL POINTS: 2000

SECURITY DOCUMENTATION

POINTS: 1300

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 and not insert any university, personal, or other identifiable information other than your team number. Security documentation must be submitted on or before November 9, 2021 at 11:59pm PST on the sCOARboard as a PDF. Late submissions will be accepted until Thursday, November 11, 2021 at 11:59PM PST to the SCOARboard. *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: 700

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 sCOARboard. Judges will be viewing your video beginning November 9. Late submissions will be accepted until Thursday, November 11, 2021 at 11:59PM PST to the SCOARboard. *Late submissions will lose 25% of the earned score*. Your video must be accessible from Tuesday, November 9 – Tuesday, November 16, 2021.

BACKGROUND:

- Your team works for Innovo Electric, the Hydropower Energy of the South.
- Innovo recently acquired Moti, a small weather analysis company.
- Your team will be provided access to Moti on Saturday, November 13 and must integrate it into Innovo's network immediately to ensure that Moti customers continue to have seamless access.
- Additionally, you will acquire the team members of Moti into your team's infrastructure.

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:

Your team is asked to submit a 5-7 minute presentation to the CEO, CIO, and COO to discuss the strategy for integration and future security. Your presentation should include

1. Your video must start with your registration 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 plan for your initial risk assessment of the blind implementation. Consider risks that would be of concern to the CEO and highlight those
3. 3-5 immediate actions you will implement to assess and better secure the system, 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 or ensure 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 system.

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) 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 12, 2021 from the White team 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
	1	2	3	4
System Overview (3%)	• Unclear definition of the system	• System defined	• System defined well	• System defined well in clear, plain language • Targets a "senior leadership" audience
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 some (<23) of the vulnerabilities provided by the "build" crew. • Most listed vulnerabilities include an appropriate mitigation	• Identified man (>22) of the vulnerabilities provided by the "build" crew. • No more than one vulnerability is missing an appropriate mitigation	• Identified most (tbd) of the vulnerabilities provided by the "build" crew. • Each vulnerability has an appropriate mitigation
System Hardening (25%)	• Hardening steps (0-1) 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	• Hardening steps (1-2) 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	• Hardening steps (3+) 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	• Hardening steps (4+) 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

C-SUITE PANEL RUBRIC

C-Suite PANEL Rubric	Emerging 1	Developing 2	Proficient 3	Exemplary 4
Summary Assessment Highlighting Plan (25%)	Summary of initial plan is missing most or all key steps or is overly detailed for a non-technical audience. Risks are not mentioned, 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 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%)	Highlights no or only non-priority actions to be taken; no reasoning for actions provided.	Highlights only 1-2 priority action (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%)	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 either clarity or reason. Argument is minimally persuasive. Resource types needed to implement are barely mentioned or are incomplete. Includes only 1 or 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. • Any additional tools or resources that are 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. • Any additional tools or resources that are 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. • Any additional tools or resources that are needed to detect, analyze, and mitigate potential vulnerabilities in the newly integrated system.
Quality of presentation (8%)	Too much of a technical approach. If visible - most of team is not dressed for a work environment and/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 and/or there are some distractions. Visual aids, slides or other materials used 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 used 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 used have professional appearance.
Presentation Time, Required elements (2%)	Did not include registration ID#, much shorter or longer than 5-7 minutes; clearly inappropriate length for amount of information expected to be shared (ideal being 5-7 minutes). Only one team member can be identified as a participant in any way.	Did not include registration ID#, longer or much shorter than 5-7 minutes; inappropriate length for amount of information expected to be shared (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 expected to be shared. 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 expected to be shared. Two or more team members participate and there is clear acknowledgement of contributions made by any absent members.

GREEN TEAM SURVEY

1. Were you able to access 10.0.TEAM_NUMBER.8:3000? If no, then please mark false for the remaining questions.	Yes	No
2. Scroll to the bottom half of the page, you should be prompted with another image and “Kuma Lake”, under Water Level, there should be a numerical value displayed.	True	False
3. In the same section, under Generators there a value of 1 or 2 should display	True	False
4. In the same section, under Generation Outflows, there should be a numerical value displayed.	True	False
5. When you click on the “Our Lakes & Dams” link, you should be presented with the following text: *InnovoEnergy has been the trusted energy resource of the south since 1989. We strive to maintain a clean and renewable energy source for all our serviceable area. Providing sustainable electricity to all our valued customers is our top priority and our pride and joy. Kuma Lake is providing our hydroelectric dam with a vast amount of power generation every year and helps to feed and regulate Lumi River.*	True	False
6. When you click on the “Recreation” link, it should open a page that outlines the following activities: • Camping • Fishing • Hiking • Swimming	True	False
7. When you click on the “Permits” link, it should open a page that outlines how to request the following permits: • Fishing Permit • Camping Permit	True	False
8. Scroll to the bottom of the page, there should only be two footer headers: About Us and Contact Us with subheadings	True	False
9. At the bottom of the page, under About Us, there should only be two links: Kuma Lake and Lumi River.	True	False
10. At the bottom of the page, under Contact Us, there should be only one link: Contact.	True	False