Presented by

Raytheon Intelligence & Space

Run by

NATIONAL CYBERWATCH CENTER

2022 MACCDC Regional Finals Team Packet

v.03-17-22 9:20pm ET

Mid-Atlantic Collegiate
Cyber Defense Competition

Table of Contents

Mid-Atlantic Collegiate
Cyber Defense Competition

Welcome

2022 marks the 17th annual running of the MACCDC, consisting of both a virtual qualifying round (February 5) and a virtual regional final (March 17-19). Full-time undergraduate and graduate degree-seeking students, representing 4-year universities and 2-year community colleges from Delaware, the District of Columbia, Maryland, New Jersey, North Carolina, Pennsylvania, Virginia, and West Virginia compete for the chance to represent the region (one of nine nationally) at the National CCDC in San Antonio, TX April 21-23. Since its inception in 2006, more than 3,500 students have participated in the MACCDC and from 2017-2020*, the MACCDC regional champion went on to win the National CCDC*.

The competition is designed to test each student team's ability to secure networked systems while maintaining standard business functionality. Each year's scenario involves team members simulating a group of employees from a fictitious company that maintains an IT infrastructure. The teams are expected to manage the systems, keep them operational, and prevent unauthorized access.

I want to say a special thanks to our sponsors (check them out on the last page). I also want to thank this year's participating schools and all the individuals and organizations that have contributed to the success of this event over the years.

Best regards,

Casey W. O'Brien
MACCDC Regional Director
National CyberWatch Center
Prince George's Community College
maccdc@nationalcyerwatch.org

Regional Final Overview

The MACCDC Regional Final is presented by Raytheon Intelligence & Space and run by the National CyberWatch Center, headquartered at the Prince George's Community College Center for Advanced Technology in Largo, Maryland.

CCDC Mission

"The goal of a Cyber Defense Competition is to provide hands-on application of information assurance skills; as such, they enhance students' understanding of both theory and practice. They provide students a laboratory in which to experiment, just as in other fields of science. They fulfill the same role as capstone projects in a traditional engineering program (i.e., projects that allow students to synthesize and integrate knowledge acquired through course work and other learning experiences into a project usually conducted in a workplace). The competition combines legal, ethical, forensics, and technical components while emphasizing a team approach. Such experiential education increases the knowledge and expertise of future professionals who may be in a position to contribute to the secure design and operation of critical information and its supporting infrastructure." *Exploring a National Cyber Security Exercise for Colleges and Universities*, Ron Dodge, Lance J. Hoffman, Daniel Ragsdale, and Tim Rosenberg, 2004.

Competition Objectives

- Build a meaningful mechanism by which institutions of higher education may evaluate their programs.
- Provide an educational venue in which students can apply the theory and skills they have learned in their course work.
- Foster a spirit of teamwork, ethical behavior, and effective communication both within and across teams.
- Open a dialog and awareness among participating institutions and students.

Mid-Atlantic Collegiate
Cyber Defense Competition

Blue Teams

The following teams will be competing in the 2022 MACCDC Regional Finals:

- Bowie State University, MD
- Capitol Technology University, MD
- Community College of Baltimore County, MD
- Drexel University, PA
- George Mason University, VA
- Liberty University, VA
- University of Maryland Baltimore County, MD
- University of Virginia, VA

The winning team will represent the Mid-Atlantic Region in the National CCDC, April 21–23 (dates subject to change). NOTE: The second-place team from the MACCDC *may* have the opportunity to compete in a Wild Card round. The winner of that round would also advance to the National CCDC.

Schedule

Friday, March 18: Day 1 Competition (all times EST):

7:45am - 8:30am	Blue Team Coach/Captain Check-In (Zoom)
8:30am - 8:50am	Opening Competition Briefing (Zoom)
9:00am - 5:00pm	Competition Day 1
11:00am - 1:00pm	C-Level Executive Meetings (Zoom)
5:00pm	Day 1 Competition Ends
5:30pm	Day 1 Debrief (Zoom)

Saturday, March 19: Day 2 Competition (all times EST):

7:45am - 8:30am	Blue Team Coach/Captain Check-In (Zoom)
8:30am - 8:50am	Morning Briefing (Zoom)
9:00am - 5:00pm	Competition Day 2
11:00am - 1:00pm	C-Level Executive Meetings (Zoom)
5:00pm	Competition Ends
7:30 - 8:30pm	Debrief and Awards Ceremony (Zoom)

Mid-Atlantic Collegiate
Cyber Defense Competition

Competition Team Identification

Throughout this document, the following terms are used:

- **Gold Team**: Competition officials who organize, run, and manage the competition. Responsibilities include, but are not limited to:
  - Administration and staffing of the event
  - Working with industry partners to orchestrate the event
  - Designing, implementing, and administering the competition infrastructure
  - Managing scoring elements and determining final standings
  - Using their authority to dismiss any team, team member, or visitor for violation of competition rules and for inappropriate and/or unprofessional conduct
  - Making provision for awards and recognition
  - Managing debrief to teams after the conclusion of the competition
  - **Main Point of Contact**:
    - Casey W. O'Brien
    - MACCDC Regional Director
    - maccdc@nationalcyberwatch.org
    - Discord [Gold Team] Casey O'Brien
- **Black Team**: Competition support members who create the competition's infrastructure, provide technical support, and provide overall administrative support to the competition. **Main Point of Contacts**: Discord:
  - [Black Team] Rob Fuller
  - [Black Team] Jake Smith
  - [Black Team] Michael Dougherty
- **White Team**: Competition officials who observe team performance in their competition area and evaluate team performance and rule compliance. White Team volunteers assess the competition team's ability to maintain their network and service availability based on a business inject and a scoring instrument, delivering inject scenarios, scoring of injects, issuing or controlling the timing of injects, etc. White Team members present in the competition room(s) assist judges by observing teams, confirming proper inject completion, reporting issues, and ensuring compliance of rules and guidelines.
- **Orange Team**: Competition volunteers that serve as end-users for the Blue Teams.
- **Blue Teams**: The institution competitive teams consisting of students competing in a CCDC event.
- **Team Captain**: A student member of the Blue Team identified as the primary liaison between the Blue Team and the White Team.
- **Team Co-Captain**: A student member of the Blue Team identified as the secondary or backup liaison between the Blue Team and the White Team, should the Team Captain be unavailable (i.e., absent from the competition room).
- **Team Representatives**: A faculty or staff representative of the Blue Team's host institution responsible for serving as a liaison between competition officials and the Blue Team's institution.
- **Red Team**: Penetration testing professionals simulating external hackers attempting to gain unauthorized access to competition teams' systems.

Mid-Atlantic Collegiate
Cyber Defense Competition

Scenario: Maritime & Transportation Systems

Over the past 17 years, the MACCDC has innovated, developed, and sought to create an original experience for not only the student teams, but all participants. Introducing scenarios that imitate real life adds a dimension of realism and fun. Past scenarios include free and secure elections, natural disasters, pandemics, healthcare, and banking, to name a few.

Fig. 1: Maritime & Transportation Systems

America's Marine Transportation System (MTS) includes waterways, ports, and moving people and goods to and from the water. MTS includes approximately:

- 25,000 miles of navigable channels
- 250 locks
- 3,500 marine terminals
- Thousands of recreational marinas, and
- The Great Lakes and St. Lawrence Seaway

Coordinating with these elements are approximately:

- 174,000 miles of rail connecting all 48 contiguous States, Canada, and Mexico
- 45,000 miles of interstate highway and 115,000 miles of supporting roadways, and
- 1,400 designated intermodal connections

According to the U.S. Department of Transportation's (DOT) Bureau of Transportation Statistics, the total value of marine freight increases significantly every decade, with ferry transport experiencing rapid growth in response to land-transport congestion and commercial fishing. Military operations also use MTS facilities, waterways, and resources. These projected trade increases also increase demands on the MTS and must be safely handled and balanced with environmental values to ensure that freight and people move efficiently to, from and on the country's waterfronts. In fact, doing so is critical to the national and economic security of the U.S. (about 99% of overseas trade enters or leaves the U.S. by ship). This waterborne cargo and associated activity contribute more than $500 billion to the U.S. Gross

Domestic Product (GDP), generates over $200 billion in annual port sector federal/state/local taxes, and sustains over 10 million jobs.

Cyber-attacks on the global MTS are not new. Complicating the matter are "too few professional mariners" and too few cybersecurity professionals. MTS entities are on heightened alert because of two recent developments: a cyber-attack impacting port operations at container terminals in several Australian ports due to a security intrusion and sabotage campaign. The impacted systems use a popular Terminal Operating System (OS) widely deployed throughout the U.S., and certain processes handled by the Terminal OS were suspended because of the cyber-attack. The attack is believed to be related to the "Death Kitty" ransomware, although full details are still not available.

The second development is the recent release of leaked Hackistanian documents detailing research into how a cyber-attack could be used to target critical infrastructure, including MTS entities. These documents cover research into topics such as using ballast water systems to sink a vessel and interfering with MTS satellite communications.

CONTAINERS R * Us

In a move to position itself as the largest player in global trade, **Container R Us** has acquired **Cyber Cargo, Inc.**, a multinational MTS organization. The official announcement was made at the Containers R Us headquarters in Wilmington, DE on February 8, 2022. The acquisition and integration of Cyber Cargo, Inc.'s research & development, software, and world-renowned personnel with Containers R Us presence at the world's largest ports was a key driver of this alliance. The process took 18 months, and the deal was signed effective February 8, 2022.

"*The acquisition of Cyber Cargo, Inc. and its related assets allows us to immediately leverage and integrate the myriad MTS-related resources, R&D, and personnel to enhance the core capabilities and preparedness of port facilities and port operators to an array of hazards, including natural and human threats*," said Jeff Jacoby, CEO, Containers R Us.

The acquisition of Cyber Cargo, Inc. fits into Containers R Us' primary objectives to double maritime trade, shrink the environmental impact of the transportation network, and support the organization's industrial core. Toward this end, specific actions are organized around the following themes including a blend of policies, programs, and projects:

- Increasing efficiency and reducing costs
- Building new markets
- Growing economic activity around the MTS and,
- Delivering results while managing for the future

Cyber Cargo INCORPORATED

Student (Blue) teams will have to balance the commercial interests and business priorities of its parent company (Container R Us), with geographical constraints, political regulation, and technical constraints, while the merging of Cyber Cargo assets with Containers R Us continues.

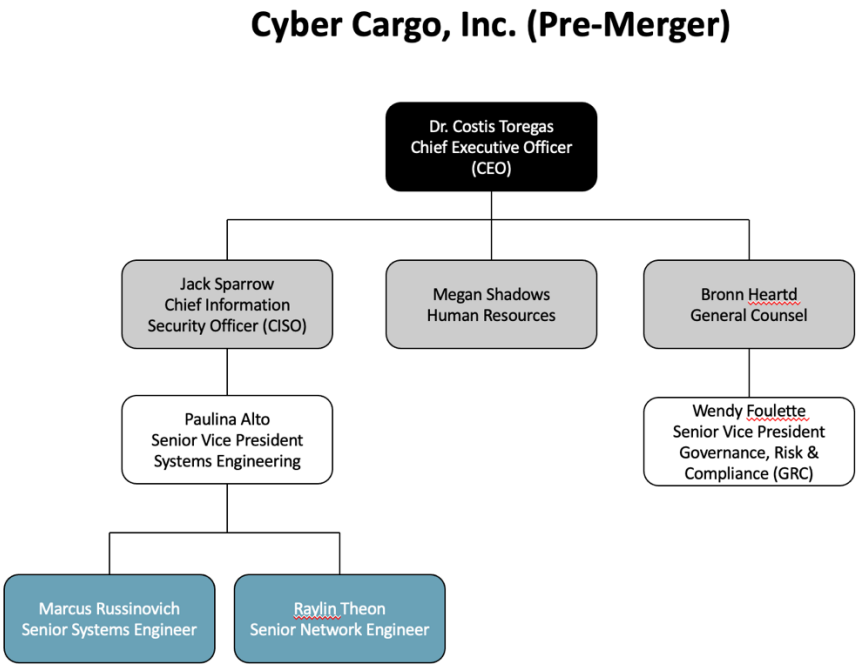

Fig. 2: Cyber Cargo, Inc. Org Chart (Pre-Merger)

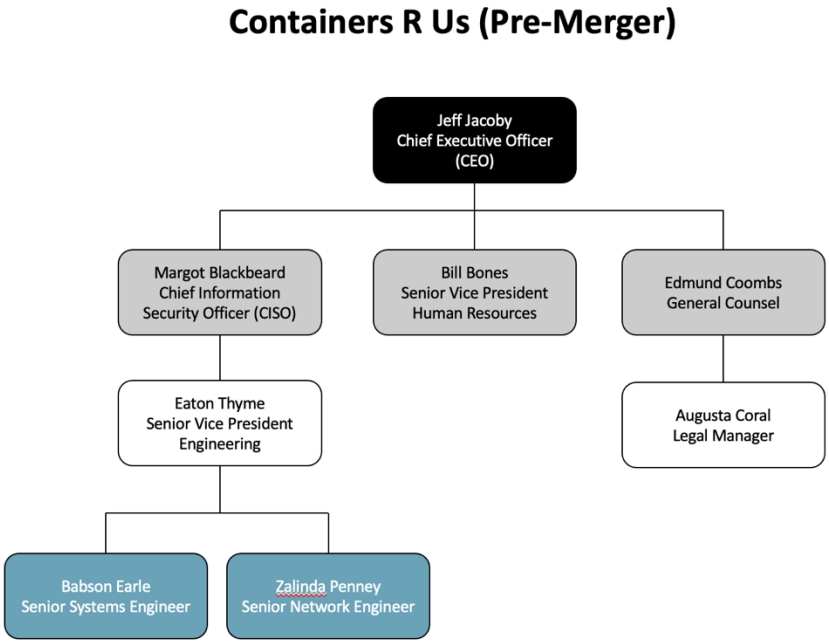

Fig. 3: Containers R Us Org Chart (Pre-Merger)

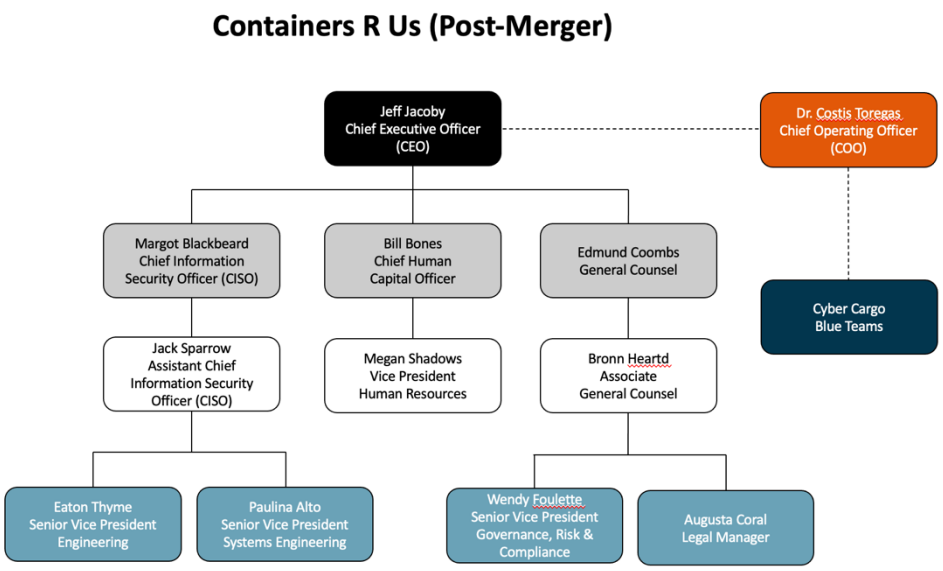

Fig. 4: Containers R Us Org Chart (Post-Merger)

Communications During the Event: Discord

Discord is the main and only communications platform allowed during the 2022 MACCDC Regional Finals (excluding Zoom, which will be used for all in/out briefs, team check-ins each morning of the competition, C-Level Executive meetings, and the Awards Ceremony). No outside teleconference platforms will be allowed. All team members are expected to join their school's designated Discord channel regardless of where the Blue team players are located. Communications with the Gold, Black, and White teams must be conducted through Discord. Be sure to check out the #readme channel once logged in for naming conventions.

Competition Rules

Competition rules are applicable to all participants of the MACCDC. They provide structure for the composition of student teams, permitted actions during competition play, guidelines for scoring, and contingencies for handling disputes. They also document expectations for appropriate conduct during the entire time participants are guests at a host site or are competing from their academic institution or other remote location. Coaches and all student participants are expected to know and follow all CCDC rules and guidelines. Access to the competition stadium environment implies their acknowledgment and their commitment to abide by them.

Coaches and team captains are responsible for deploying the competition rules to the remaining members of their team. Host sites reserve the right to stipulate additional rules conforming to local policies and guidelines.

Source: https://www.nationalccdc.org/index.php/competition/competitors/rules

1. **Competitor Eligibility**
    a. Competitors in CCDC events must be full-time students of the institution they are representing.
        i. Team members must qualify as full-time students as defined by the institution they are attending.
        ii. Individual competitors may participate in CCDC events for a maximum of five seasons. A CCDC season is defined as the period of time between the start of the first state event and the completion of the National CCDC event. Participation on a team in any CCDC event during a given season counts as participation for that entire season.
        iii. A competitor in their final semester prior to graduation is exempt from the full-time student requirement and may compete in CCDC events as a part-time student provided the competitor has a demonstrated record of full-time attendance for the previous semester or quarter.
        iv. If a team member competes in a qualifying, state, or regional CCDC event and graduates before the next CCDC event in the same season, that team member will be allowed to continue to compete at CCDC events during the same season should their team win and advance to the next round of competition.
    b. Competitors may only be a member of one team per CCDC season.
    c. A team member may not participate in any role at CCDC events held outside the region in which their team competes during the same CCDC season.
    d. Individuals who have participated in previous CCDC events in any role other than as a competitor must obtain eligibility approval from the director of the region in which their team competes prior to being added to the team roster. Once a candidate's eligibility has been approved, they will remain eligible for all CCDC events during the same season.

2. **Team Composition**
    a. Each team must submit a roster of up to 12 competitors to the designated registration system. Rosters must be submitted by published deadlines and include a coach who is a staff or faculty member of the institution the team is representing. All competitors on the roster must meet all stated eligibility requirements. No changes to the team roster will be permitted after the team competes in their first CCDC event. The competition team must be chosen from the submitted roster. A competition team is defined as the group of individuals competing in a CCDC event.
    b. Each competition team may consist of up to eight (8) members chosen from the submitted roster.
    c. Each competition team may have no more than two (2) graduate students as team members.
    d. If the member of a competition team advancing to a qualifying, state, regional, or national competition is unable to attend that competition, that team may substitute another student from the roster in their place prior to the start of that competition.

e. Once a CCDC event has begun, a team must complete the competition with the team that started the competition. Substitutions, additions, or removals of team members are prohibited except for extreme circumstances.
f. Team Representatives must petition the Competition Director in writing for the right to perform a change to the competition team.
g. The Competition Director must approve any substitutions or additions prior to those actions occurring.
h. Teams or team members arriving after an event's official start time, for reasons beyond their control, may be allowed to join the competition provided a substitution has not already been made. Event coordinators will review the reason for tardiness and make the final determination.
i. Each team will designate a Team Captain for the duration of the competition to act as the team liaison between the competition staff and the teams before and during the competition. In the event of the Team Captain's absence, teams must have an identified team liaison serving as the captain in the competition space at all times during competition hours.
j. An institution is only allowed to compete one team in any CCDC event or season.
k. A CCDC team may only compete in one region during any given CCDC season.
l. Exhibition teams are not eligible to win any CCDC event and will not be considered for placement rankings in any CCDC event.

3. Team Representatives

a. Each team must have at least one representative present at every CCDC event. The representative must be a faculty or staff member of the institution the team is representing.
b. Once a CCDC event has started, representatives may not coach, assist, or advise their team until the completion of that event (including overnight hours for multi-day competitions).
c. Representatives may not enter their team's competition space during any CCDC event.
d. Representatives must not interfere with any other competing team.
e. The representative, or any non-team member, must not discuss any aspect of the competition event, specifically event injections, configurations, operations, team performance or red team functions, with their team during CCDC competition hours and must not attempt to influence their team's performance in any way.
f. Team representatives/coaches may not participate on the Red Team, Gold Team, Operations Team, Black Team, White Team, or Orange Team at any CCDC event.

4. Competition Conduct

a. Throughout the competition, Black, White and Orange Team members will occasionally need access to a team's system(s) for scoring, troubleshooting, etc. Teams must immediately allow these Team members' access when requested.
b. Teams must not connect any devices or peripherals to the competition network unless specifically authorized to do so by the Black or White Team members.
c. Teams may not modify the hardware configurations of competition systems. Teams must not open the case of any server, printer, PC, monitor, KVM, router, switch, firewall,

or any other piece of equipment used during the competition. All hardware related questions and issues should be referred to the White Team.

d. Teams may not remove any item from the competition area unless specifically authorized to do so by the Black or White Team members including items brought into the team areas at the start of the competition.
e. Team members are forbidden from entering or attempting to enter another team's competition workspace or room during CCDC events.
f. Teams must compete without "outside assistance" from non-team members including team representatives from the start of the competition to the end of the competition (including overnight hours for multi-day events). All private communications (calls, emails, chat, texting, directed emails, forum postings, conversations, requests for assistance, etc.) with non-team members including team representatives that would help the team gain an unfair advantage are not allowed and are grounds for disqualification and/or a penalty assigned to the appropriate team.
g. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.
h. Team representatives, Remote Site Judges, sponsors, and observers are not competitors and are prohibited from directly assisting any competitor through direct advice, "suggestions", or hands-on assistance. Any team sponsor or observers found assisting a team will be asked to leave the competition area for the duration of the competition and/or a penalty will be assigned to the appropriate team.
i. Team members will not initiate any contact with members of the Red Team during the hours of live competition (unless permitted via a public Discord channel). Team members are free to talk to Red Team members during official competition events such as breakfasts, dinners, mixers, and receptions that occur outside of live competition hours.
j. Teams are free to examine their own systems but no offensive activity against any system outside the team's assigned network(s), including those of other CCDC teams, will be tolerated. Any team performing offensive activity against any system outside the team's assigned network(s) will be immediately disqualified from the competition. If there are any questions or concerns during the competition about whether specific actions can be considered offensive in nature contact the Black Team before performing those actions.
k. Teams are allowed to use active response mechanisms such as TCP resets when responding to suspicious/malicious activity. Any active mechanisms that interfere with the functionality of the scoring engine or manual scoring checks are exclusively the responsibility of the teams. Any firewall rule, IDS, IPS, or defensive action that interferes with the functionality of the scoring engine or manual scoring checks are exclusively the responsibility of the teams.
l. All team members will wear badges identifying team affiliation at all times during competition hours.
m. Only Black and White Team members will be allowed in competition areas outside of competition hours.

5. Internet Usage

a. Internet resources such as FAQs, how-to's, existing forums and responses, and company websites, are completely valid for competition use provided there is no fee required to access those resources and access to those resources has not been granted based on a previous membership, purchase, or fee. Only resources that could reasonably be available to all teams are permitted. For example, accessing Cisco resources through a CCO account would not be permitted but searching a public Cisco support forum would be permitted. Public sites are acceptable. Only public resources that every team could access if they chose to are permitted.

b. Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition. Teams are not allowed to access private Internet-accessible libraries, FTP sites, web sites, network storage, email accounts, or shared drives during the competition. All Internet resources used during the competition must be freely available to all other teams. The use of external collaboration and storage environments such as Google Docs/Drive is prohibited unless the environment was provided by and is administered by competition officials. Accessing private staging areas or email accounts is grounds for disqualification and/or a penalty assigned to the appropriate team.

c. No peer to peer or distributed file sharing clients or servers are permitted on competition networks unless specifically authorized by the competition officials.

d. Internet activity, where allowed, will be monitored and any team member caught viewing inappropriate or unauthorized content will be subject to disqualification and/or a penalty assigned to the appropriate team. This includes direct contact with outside sources through chat/email or any other public or non-public services including sites (e.g., Facebook). For the purposes of this competition inappropriate content includes pornography or explicit materials, pirated media files, sites containing key generators and pirated software, etc. If there are any questions or concerns during the competition about whether specific materials are unauthorized contact the White Team immediately.

e. All network activity that takes place on the competition network may be logged and subject to release. Competition officials are not responsible for the security of any information, including login credentials, which competitors place on the competition network.

f. Scripts, executables, tools, and programs written by active team members may be used in CCDC events provided:

    i. The scripts, executables, tools, and programs have been published as a publicly available resource on a public and non-university affiliated site (e.g., GitHub) for at least 3 months prior to their use in any CCDC event.

    ii. Teams must send the public links and descriptions of the team-written scripts, executables, tools, and programs to the appropriate Competition Director at least 30 days prior to their use in any CCDC event. Development must be “frozen” at time of submission with no modifications or updates until after the team competes in their last CCDC event of that season.

    iii. Teams must consent to the distribution of the submitted links and descriptions to all other teams competing in the same CCDC event

where the team-written scripts, executables, tools, and programs will be used.

iv. Team written tools, scripts, or executables that use resources outside of the competition environment other than simple DNS lookups are prohibited (e.g., tools that use cloud services or cloud processing outside of the competition environment are prohibited).

v. Team written tools, scripts, or executables that transmit data outside of the competition environment (e.g., log data) must be declared to competition officials at least 30 days prior to their use in any CCDC event. Teams must obtain written authorization from competition officials prior to using these tools in any CCDC event. Approval or rejection of these tools is at the sole discretion of competition officials.

6. Permitted Materials

a. No memory sticks, flash drives, removable drives, CDROMs, electronic media, or other similar electronic devices are allowed in the room during the competition unless specifically authorized by the Operations or White Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.

b. Teams may not bring any type of computer, laptop, tablet, smart phone, or wireless device into the competition area unless specifically authorized by the Black Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.

c. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition as specified by the competition officials.

7. Professional Conduct

a. All participants, including competitors, coaches, White Team, Red Team, Black Team, Orange Team, and Gold Team members, are expected to behave professionally at all times during all CCDC events including preparation meetings, receptions, mixers, banquets, competitions, and so on.

b. In addition to published CCDC rules, Host Site policies and rules apply throughout the competition and must be respected by all CCDC participants.

c. All CCDC events are alcohol free events. No drinking is permitted at any time during competition hours.

d. Activities such as swearing, consumption of alcohol or illegal drugs, disrespectful or unruly behavior, sexual harassment, improper physical contact, becoming argumentative, willful violence, or willful physical damage have no place at the competition and will not be tolerated.

e. Violations of the rules can be deemed unprofessional conduct if determined to be intentional or malicious by competition officials.

f. Competitors behaving in an unprofessional manner may receive a warning from the Gold/Black/White Teams for their first offense. For egregious actions or for subsequent violations following a warning, competitors may have a penalty assessed against their

team, be disqualified, and/or expelled from the competition site. Competitors expelled for unprofessional conduct will be banned from future CCDC competitions for a period of no less than 12 months from the date of their expulsion.

g. Individual(s), other than competitors, behaving in an unprofessional manner may be warned against such behavior by the Gold/Black/White Teams or asked to leave the competition entirely by the Competition Director.

8. Questions, Disputes, and Disclosures

a. PRIOR TO THE COMPETITION: Team captains are encouraged to work with the Competition Director and their staff to resolve any questions regarding the rules of the competition or scoring methods before the competition begins.

b. DURING THE COMPETITION: Protests by any team must be presented in writing by the Team Captain to the Competition Director as soon as possible. The competition officials will be the final arbitrators for any protests or questions arising before, during, or after the competition. Rulings by the competition officials are final. All competition results are official and final as of the Awards/Closing Ceremony.

c. In the event of an individual disqualification, that team member must leave the competition area immediately upon notification of disqualification and must not re-enter the competition area at any time. Disqualified individuals are also ineligible for individual or team awards.

d. In the event of a team disqualification, the entire team must leave the competition area immediately upon notice of disqualification and is ineligible for any individual or team award.

e. All competition materials including injects, scoring sheets, and team-generated reports and documents must remain in the competition area. Only materials brought into the competition area by the student teams may be removed after the competition concludes.

9. Scoring

a. Scoring will be based on keeping required services up, controlling/preventing unauthorized access, and completing business tasks that will be provided throughout the competition. Teams accumulate points by successfully completing injects and maintaining services. Teams lose points by violating service level agreements, usage of recovery services, and successful penetrations by the Red Team.

b. Scores will be maintained by the competition officials and may be shared at the end of the competition. There will be no running totals provided during the competition. Team rankings may be provided at the beginning of each competition day.

c. Any Blue Team action that interrupts the scoring system is exclusively the responsibility of that team and will result in a lower score. Any Blue Team member that modifies a competition system or system component, with or without intent, in order to mislead the scoring engine into assessing a system or service as operational, when in fact it is not, may be disqualified and/or the team assessed penalties. Should any question arise about scoring, the scoring engine, or how scoring functions, the Team Captain should immediately contact the competition officials to address the issue.

d. Teams are strongly encouraged to provide incident reports for each Red Team incident they detect. Incident reports can be completed as needed throughout the competition and presented to the White Team for collection. Incident reports must contain a description of what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, access obtained, damage done, etc.), a discussion of what was affected, and a remediation plan. A thorough incident report that correctly identifies and addresses a successful Red Team attack may reduce the Red Team penalty for that event - no partial points will be given for incomplete or vague incident reports.

10. Remote/Team Site Judging and Compliance

With the advent of viable remote access technologies and virtualization, teams will have the ability to participate in CCDC events from their respective institutions. This section addresses policy for proper engagement in CCDC events for remote teams.

a. One or more Remote Site Judge(s) must be assigned to the team site. At least one Remote Site Judge must be present at the remote site for the duration of the event to facilitate the execution of the CCDC. The qualifications of Remote Site Judge are the same as Event Judge.
b. Subject to the specifications of the remote competition, the responsibilities of the Remote Site Judge may include the following:
    i. Be present with the participating team to assure compliance with all event rules
    ii. Provide direction and clarification to the team as to rules and requirements
    iii. Establish communication with all Event Judges and provide status when requested
    iv. Provide technical assistance to remote teams regarding use of the remote system
    v. Review all equipment to be used during the remote competition for compliance with all event rules
    vi. Assure that the Team Captain has communicated to the Event Judges approval of initial system integrity and remote system functionality
    vii. Assist Event Judges in the resolution of grievances and disciplinary action, including possible disqualification, where needed
    viii. Report excessive misconduct to local security or police
    ix. Assess completion of various injects based on timeliness and quality when requested by Event Judges
    x. Act as a liaison to site personnel responsible for core networking and internet connectivity
    xi. Provide direct technical assistance to teams when requested by Event Judges
    xii. Provide feedback to students after the completion of the CCDC event
c. A recommendation for Remote Site Judge(s) is expected to be given from a Team representative of the participating institution to the CCDC Event Manager. Remote Site Judge(s) must not be currently employed, a student of, or otherwise affiliated with the participating institution, other than membership on an advisory board. CCDC Event Managers should also be apprised of a contact from the participating institution responsible for core networking and internet connectivity that will be available during the CCDC event. Remote teams are required to compete from a location with controlled

access (e.g., a separate room or a portion of a room that is dedicated for use during the CCDC event). Workstations and internet access must comply with published requirements.

Scoring

All Blue Teams start with zero points. Blue Teams are ranked against each other in order of highest (best) to lowest score.

Scoring Metrics:

1. **Services**: All scored services must remain up and available, with a high degree of integrity. All services are given a predefined point value and will be checked periodically using Service Round Checks. The actual number of Service Rounds is not disclosed prior to or during the competition. For each service that passes the necessary check, the team will receive the appropriate number of points for that service. The more service points a team receives, the better.

    a. **Recovery Services**: In the event of system lock or failure, teams can request that a virtual machine (VM) be reset to a known good state (revert to snapshot). Teams are allowed two (2) free reverts total for the entire event, per team. Each additional request for a VM snapshot revert will carry a 10% point penalty in the total service score for the event.

    b. **Service-Level Agreements**: Each failed check of a service carries a 10% point penalty of the service's maximum point value assessed on the next successful check of that service, up to a maximum of a 50% penalty. Each successful service check mitigates a single 10% point penalty until 100% is restored. For example:
        a. Service a: 100 points (up), 0 points (down), 0 points (down), 80 points (up), 90 points (up), 0 points (down), 80 points (up), 0 points (down), 0 points (down), 0 points (down), 0 points (down), 0 points (down), 50 points (up), 60 points (up)
        b. Service b: 100 points (up), 100 points (up), 0 points (down), 0 points (down), 80 points (up), 90 points (up), 100 points (up), 100 points (up), 100 points (up), 100 points (up), 100 points (up), 0 points (down), 90 points (up), 0 points (down)

2. **Injects**: Throughout the competition, the Blue Team will be presented with injects. An inject is any assigned task to be completed in the assigned amount of time. Inject types vary and are weighted based on the difficulty and time sensitivity of the task. Tasks may contain multiple parts. Sample injects include creating policy documents, making technical changes to a system, and attending meetings. Injects can be delivered through any number of methods, including electronically and orally. Injects will be scored by a White Team member. If the inject is completed on time and to the standard required, the Blue Team will receive the appropriate number of points. Unless indicated otherwise, the Team Captain may assign injects to specific team members for completion. Red Team activity can adversely affect a team's ability to complete injects. It is the Blue Teams' responsibility to keep their systems available. No extra

time or point credit will be given for injects that are not completed because of inability to access a system. The more inject points a team receives, the better.

3. **Red Team Activity**: The activities performed by the Red Team have an impact on many of the scoring categories. It is imperative that Blue Teams work to prevent Red Team activities. The Red Team will have specific goals during the event, such as compromising a server, stealing data, and modifying injects. All Red Team activities are meant to disrupt or misinform. At the conclusion of each competition day, the Red Team will rank order each team from best to worst.

4. **C-Level Executive Meetings**: Each Team Captain will meet face-to-face with various Containers R Us C-Level executives (see the schedule below). During the initial meeting on Day 1 (10 minutes, timed), these executives will expect to be briefed on the status of the organization's information systems, the number of users impacted by downed systems, as well other items the Team Captain considers relevant for them to know. At this initial meeting, each Team Captain will be given action items to complete within a fixed time. Items may include a written status report, a high-level remediation plan, a resource inventory, a request for prioritized additional resources subject to budget constraints, and other similar management considerations. The more points a team receives, the better.

   Day 1 C-Level Executive Meeting Schedule:
   - 11:00am: Bowie State University
   - 11:15am: Capitol Technology University
   - 11:30am: Community College of Baltimore County
   - 11:45am: Drexel University
   - 12:00pm: George Mason University
   - 12:15pm: Liberty University
   - 12:30pm: University of Maryland Baltimore County
   - 12:45pm: University of Virginia

   During the second meeting on Day 2 (10 minutes, timed), each Team Captain will meet again with various C-Level executives and have a chance to present responses to what was covered in the Day 1 meeting and provide updates on any changes that transpired.

   Day 2 C-Level Executive Meeting Schedule:
   - 11:00am: Bowie State University
   - 11:15am: Capitol Technology University
   - 11:30am: Community College of Baltimore County
   - 11:45am: Drexel University
   - 12:00pm: George Mason University
   - 12:15pm: Liberty University
   - 12:30pm: University of Maryland Baltimore County
   - 12:45pm: University of Virginia

Each team will be scored using the following metrics:

- Oral presentation and writing skills
- Clarity of communicating the situation
- Ability to rise above technobabble
- Creativity in reacting to new information

5. **Incident Response**: All Blue Teams must submit a minimum of 4 Incident Response reports (and no more than 8) over the course of the 2 days of competition to the Incident Response officials (they are part of the White Team). Each team's 4 best IR reports will be averaged to determine the Blue Team's IR raw score (if a Blue Team submits less than 4 reports, the one(s) not submitted will be scored as zero points). Blue Teams will then be ranked from first through eighth place based on their averaged raw score.

   A link to download a .PDF version of the Incident Response form was provided in the #competition-announcements channel in Discord. Instructions for submitting these forms will be provided during the initial team briefing on Day 1. IR reports will be scored based on coherence and technical accuracy. A thorough report that correctly identifies and addresses a successful Red Team attack may reduce the penalty for that event. No partial points will be given for incomplete or vague incident reports. While not required, teams can ask for two (2) consultations to help in report writing (it's better to ask for these consultations on Day 1, as Day 2 gets extremely busy).

Calculating Scores:

- All Blue Teams start with zero points.
- Raw scores are used for the scoring metrics, excluding the Red Team (which uses an ordinal scale, see next).
- Blue Teams are ranked using an ordinal scale, which is a measurement scale that assigns values to objects based on their ranking with respect to one another. For example, a first-place finish in the service-scoring metric warrants an ordinal score of 1, a second-place finish warrants an ordinal score of 2, up to an eighth-place finish warranting an ordinal score of 8. This process is repeated for all the scoring metrics.
- The ordinal scores from all the scoring metrics from both days are then totaled for each Blue Team, yielding a combined ordinal score, which is used to rank the Blue Teams from first through eighth place. The winning Blue Team will be determined based on the lowest combined ordinal score obtained during the competition time.
- In the event of a tie for first place, the team with the highest raw combined inject and service score will win.

Competition Topology

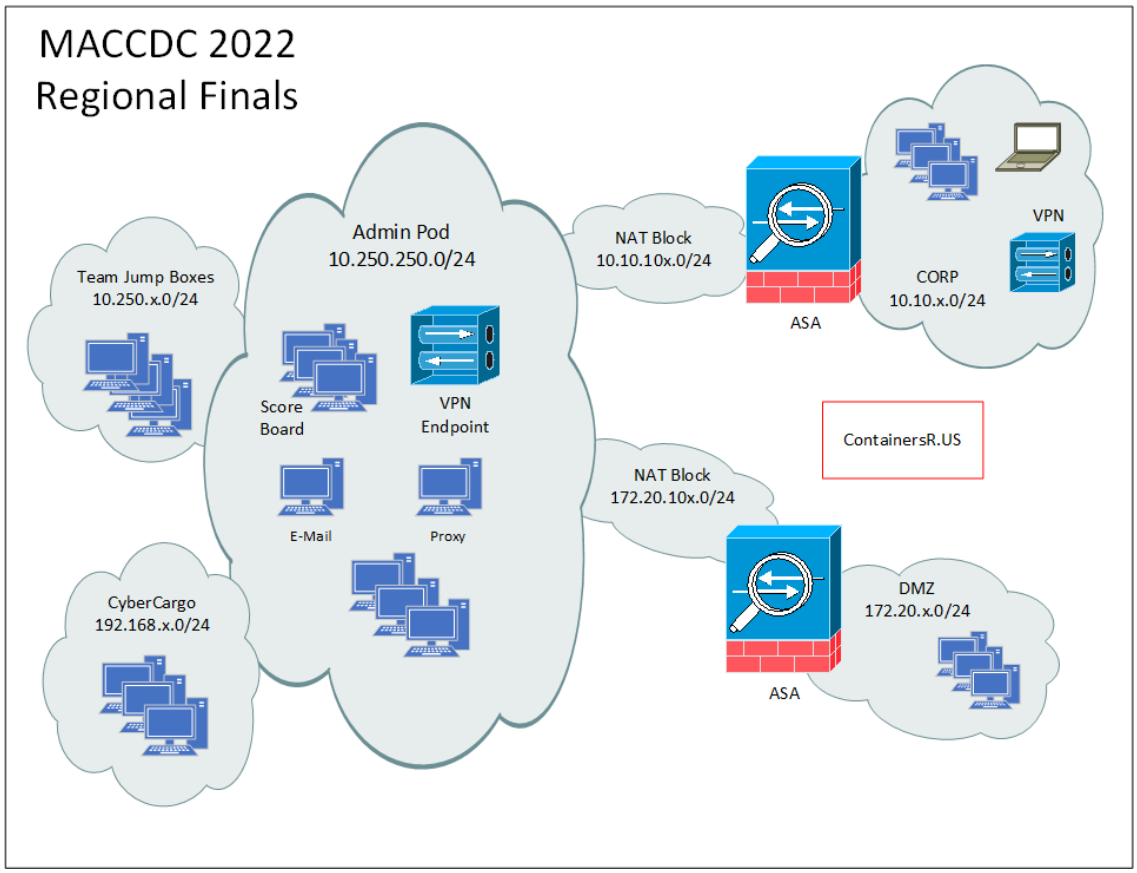

Fig. 5: Competition Network Topology

AWS Jump Boxes		
IP Range	**OS**	**Functionality**
10.250.x.0/24	**Win Server 2019: 4 total**	**Remote Desktop Protocol (RDP)**
	Ubuntu 20.04: 4 total	**Virtual Network Computing (VNC)**

Table 1: AWS Jump Box Table

Container R Us Corp Network: 10.10.x.0/24 (corp.teamX.containersr.us)				
Hostname	**IP Addr**	**NAT IP Addr**	**OS**	**Scored Services**
pdc	10.10.X.10	10.10.10X.10	Windows Server 2012 R2	389, 445, 3389, 5985
sdc	10.10.X.11	10.10.10X.11	Windows Server 2016	389, 445, 3389, 5895
ca	10.10.X.22	10.10.10X.22	Windows Server 2016	443, 445, 5985
edr	10.10.X.50	10.10.10X.50	Amazon Linux 2	443, 9200
db1	10.10.X.55	10.10.10X.55	Windows Server 2012 R2	3306, 5432
salt	10.10.X.114	10.10.10X.114	Amazon Linux 2	22. 2049, 443
opengts	10.10.X.143	10.10.10X.143	Ubuntu 18.04	22, 2049, 80
gogs	10.10.X.160	10.10.10X.160	Fedora 33	22, 80, 2375
siem	10.10.X.200	10.10.10X.200	Ubuntu 20.04	INJECT LATER (443)
vpn	10.10.X.202	10.10.10X.202	Palo Alto	INJECT LATER (ICMP)
wk1	10.10.X.218	10.10.10X.218	Windows Server 2012 R2	Orange Team
wk2	10.10.X.221	10.10.10X.221	Windows Server 2012 R2	Orange Team
wk3	10.10.X.231	10.10.10X.231	Windows Server 2019	Orange Team
wk4	10.10.X.238	10.10.10X.238	Windows Server 2019	Orange Team
inspector	10.10.X.250	N/A	Ubuntu 20.04	White Team Only
corp-asa	10.10.X.254	10.10.10X.254	Cisco ASA	N/A

Table 2: Containers R Us Corporate Network

NOTE: Blue Teams will not have access to the workstation boxes (wkX)

Container R Us DMZ 172.20.x.0/24 (dmz.teamX.containersr.us)				
Hostname	**IP Addr**	**NAT IP Addr**	**OS**	**Scored Services**
dc1	172.20.X.20	172.20.10X.20	Windows Server 2016	389, 445, 3389
dc2	172.20.X.30	172.20.10X.30	Windows Server 2012 R2	389, 445, 3389
control	172.20.X.100	172.20.10X.100	Ubuntu 18.04	2049, 10250
node1	172.20.X.110	172.20.10X.110	Ubuntu 18.04	10250
node2	172.20.X.120	172.20.10X.120	Ubuntu 20.04	21, 10250
node3	172.20.X.130	172.20.10X.130	Fedora 33	10250
mq	172.20.X.207	172.20.10X.207	Fedora 33	443, 61616
dmz-asa	172.20.X.254	172.20.10X.254	Cisco ASA	N/A

Table 3: Containers R Us DMZ

CyberCargo Network 192.168.x.0/24 (teamX.cybercargo.net)			
Hostname	IP Addr	OS	Scored Services
dc01	192.168.X.10	Windows Server 2012 R2	389, 445, 3389
dc02	192.168.X.20	Windows Server 2019	389, 445, 3389
gocd	192.168.X.32	Red Hat 8	22, 8153
git	192.168.X.41	openSUSE Leap 15.2	22, 443
gts	192.168.X.44	Ubuntu 18.04	21, 22, 443
rmq	192.168.X.71	openSUSE Leap 15.2	22, 2049, 443
cfe	192.168.X.83	CentOS 7	22, 80, 443
ws1	192.168.X.123	Windows Server 2016	Orange Team
ws2	192.168.X.158	Windows Server 2016	Orange Team
ws3	192.168.X.192	Windows Server 2016	Orange Team
ws4	192.168.X.204	Windows Server 2016	Orange Team
ws5	192.168.X.227	Windows Server 2016	Orange Team

Table 4: CyberCargo Network

NOTE: Blue Teams will not have access to the workstation boxes (wsX)

Functional Services

In addition to being up and accepting connections, the services must be functional and serve the intended business purpose. At random intervals, the following services (*subject to change*) will be tested for functionality and content where appropriate:

DNS
Domain Name System (DNS). DNS lookups will be performed against the DNS server. Each successfully served request will be awarded points.

Elasticsearch
On port 9200, an unauthenticated query is performed on the index and an expected result is determined. The check is then completed.

FTP
A /dev/random generated file is attempted to be uploaded via an FTP logged in session and that same file is attempted to be downloaded and verified that it's the same hash as the one that is uploaded. This check is then completed.

HTTP
Hypertext Transfer Protocol (HTTP). A request for a specific web page will be made. Once the request is made, the result will be stored in a file and compared to the expected result. The returned page must match the expected content for points to be awarded.

HTTPS
Hypertext Transfer Protocol Secure (HTTPS). A request for a page over SSL will be made. Again, the request will be made, the result stored in a file, and the result compared to the expected result. The returned page needs to match the expected file for points to be awarded.

LDAP
Lightweight Directory Access Protocol (LDAP). An authenticated query to the Active Directory LDAP service will be performed. Each successfully performed query will be awarded points.

Kerberos
A user will need to connect and successfully authenticate using Kerberos authentication.

MySQL
MySQL (Database). A connection to the database will be made with a specified user and a query will be run. The output of the query will be compared and each correctly answered query will be awarded points.

NFS
An NFS export is mounted and checked for a number of different specified files. These files are then checked for integrity and the check is completed.

PostgreSQL
An authenticated SQL query is performed against the database and an expected outcome is recorded and checked. This check is then completed.

RDP
Remote Desktop (RDP). A specified user will attempt to log in via RDP to the service. This will simulate an employee working from home. If a desktop appears, the check will be successful. Each successful test of RDP functionality will be awarded points.

SMB
Server Message Block (SMB). A specified user will attempt to connect to and read a designated file from the remote host. This file will then be hashed and compared against the expected value. This will simulate an employee accessing shares on the network. Each successful file read, and integrity test will be awarded points.

SSH
Secure Shell (SSH). A connection to the server will be made with a specified user, and commands will be executed as that user. The output of the commands and the ability to connect will be scored, with points awarded upon successful execution.

WinRM
An authenticated WinRM session is connected and a PowerShell command is run. The outcome of this command is recorded and checked. This check is then completed.

Initial Connection

There are two (2) separate systems that are used to provide the services and scoring necessary to meet the goals of the MACCDC:

System 1, AWS Jump Boxes: This is how teams access the competition network. Teams will access an Apache Guacamole Web interface in their browsers, which lets them connect over both RDP for GUI access to Windows jump hosts, as well as VNC to the Linux jump hosts.

IP addresses, usernames, and passwords for the Jump Hosts/Guacamole portal will be provided prior to the competition for connectivity testing via the private Discord channels for each team.

System 2, Scoreboard. This will only be accessible (via a browser) internally to the competition network.

Usernames and passwords for the Scoreboard will be provided prior to the competition via the private Discord channels for each team.

Tech Support/Ticketing System

The Black Team relies on a custom-built Ticketing System integrated in Discord to support the Blue Teams during the competition. Team Captains should be the only ones submitting tickets. Syntax:

- Open a new ticket: *-tickets Open/create/new/make*
- Add a user to the ticket in this channel: *-tickets AddUser*
- Remove a user from the ticket: *-tickets RemoveUser*
- Rename a ticket: *-tickets Rename*
- *Close a ticket: -tickets Close/end/delete*

Systems

1. Each Blue Team will start the competition with identically configured systems.
2. Blue Teams may not add or remove any computer, printer, or networking device from the designated competition area (where applicable).
3. Blue Teams should not assume any competition system is properly functioning or secure.
4. Network traffic generators may be used throughout the competition to generate traffic on each team's network. Traffic generators may generate typical user traffic as well as suspicious or potentially malicious traffic from random source IP addresses throughout the competition.
5. Blue Teams must maintain specific services on the "public" IP addresses assigned to their team and stipulated in this document. Moving services from one public IP to another is not permitted unless directed to do so by an inject or the Black Team. Likewise, Blue teams are not permitted to change the internal addressing or Virtual Local Area Networking (VLAN) scheme of the competition network unless directed to do so by an inject or the Black Team.
6. Blue Teams may re-task servers, moving a service from one server to another as long as the outside "public" IP address of the service remains the same. It is the responsibility of the Blue Teams to understand all the particulars of scoring a service when doing so.

7. Blue Teams are not permitted to alter the system names or IP address of their assigned systems unless directed by an inject or the Black Team; this may affect the results of the scoring mechanism.
8. Systems designated as user workstations within the competition network(s) are to be treated as user workstations and may not be re-tasked for any other purpose by the Blue Teams.
9. Blue Teams may not modify the hardware configurations of workstations used to access the competition network.
10. Servers and networking equipment may be re-tasked or reconfigured as needed.
11. Red Team activity will be active throughout the event. At no time will the Red Team have access outside the network perimeter(s).
12. Each Blue Team network will be monitored by a scoring system. An indication of services, as viewed by the indigenous scoring engine, may be made available to each Blue Team via a Scoreboard webpage.
13. While every effort is made to provide a stable and well-defined competition topology, it is subject to change and/or modification as decided by the MACCDC Regional Director and Black Team.

Questions and Disputes

Team captains are encouraged to work with the local site judge and contest staff to resolve any questions or disputes regarding the rules of the competition or scoring methods before the competition begins. Protests by any team will be presented by the Team Captain to the competition officials as soon as possible. Competition Gold Team officials will be the final arbitrators for any protests or questions arising before, during, or after the competition, and rulings by the competition officials are final.

In the event of an individual disqualification, that team member must leave the competition area immediately upon notification of disqualification and must not re-enter the competition area at any time. Disqualified individuals are also ineligible for individual awards or team trophies.

In the event of a team disqualification, the entire team must leave the competition area immediately upon notice of disqualification and is ineligible for any individual or team award.

Aftermath

Members of the MACCDC Gold, White, and Red Teams strive to make the MACCDC an enriching experience. All management and administrative teams are open to feedback and suggestions for improvement after the completion of the competition. This may include areas of concern or dissatisfaction.

Whether feedback is positive or negative, participants are forbidden from publishing, posting on the Internet, or publicly communicating details of the competition other than what is available at www.nationalccdc.org or maccdc.org.

Institutions that fail to adhere to this rule may be refused participation in future competitions. Institutions may publish, post on the Internet, or publicly communicate news stories of a general nature about the MACCDC, and may also enumerate participating teams and winners.

Errata

Date/Time (all times EST):

- 02-22:
  - 10:02am:
    - Misc. formatting
  - 9:00pm:
    - Page 3: Updated Table of Contents
    - Page 11: Updated Discord section
    - Page 19: Moved Recovery Services and Service Level Agreements under Services section
    - Page 20: #5, Recovery Services changed to, “Teams are allowed two (2) free reverts total for the entire event, per team.”
    - Pages 22-24: added Elasticsearch, Microsoft SQL, and PostgreSQL to list of Functional Services and alphabetized them
- 02-28:
  - 2:34pm:
    - Page 1: Added banner image
  - 2:50pm:
    - Page 8: Added Containers R Us and Cyber Cargo Inc. logos
- 03-08:
  - 8:00pm:
    - Page 21: Added Fig. 5 Competition Network Diagram
    - Page 23: Added FTP, NFS, and WinRM to Functional Services list
- 03-14:
  - 7:58pm:
    - Pages 21-22: Removed Tables 1-3; replaced with Figures 6-8
    - Page 22: Removed Docker and Microsoft SQL Server from Functional Services list
- 03-15:
  - 6:58pm:
    - Pages 22-24: Updated Figures 6-8

- 03-16:
  - 8:53pm:
    - Title Page: Added Raytheon and National CyberWatch logos
    - Pages 22-24: Removed Figures 6-8 and replaced with Tables 1-3

- 03-17:
  - 11:10am:
    - Page 23: Table 4: Changed hostname *cfe* from Rocky Linux 8 to CentOS 7 and changed its scored services from 22, 80 to 22, 80, 443
  - 12:35pm:
    - Pages 23-24: Functional Services section: Updated how check works for Elasticsearch, FTP, NFS, PostgreSQL, and WinRM
  - 4:25pm:
    - Page 22: Table 3: Changed hostname *node1* from Debian 10 to Ubuntu 18.04
  - 9:20pm:
    - Page 20: Updated Incident Response section.