MACCDC 2021

Presented by: Raytheon Intelligence & Space Mid-Atlantic Collegiate Cyber Defense Competition

16th Annual Mid-Atlantic Collegiate Cyber Defense Competition

TABLE OF CONTENTS

WELCOME

What a year is the understatement of, well, the year. And speaking of years, 2021 marks the 16th annual MACCDC, consisting of both a virtual qualifying round and a virtual regional final engaging 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. Since its inception in 2006, more than 3500 students have participated in the MACCDC.

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 maintain an IT infrastructure. The teams are expected to manage the systems, keep them operational, and prevent unauthorized access. The winner of the MACCDC represents our region in the National CCDC, April 23–25 (also virtual this year). The past four (in a row) National CCDC champions have come from the MACCDC region!

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 of the individuals and organizations that have contributed to the success of this event over the years.

Best regards,

Casey W. O'Brien
Executive Director and Co-Principal Investigator
MACCDC Regional Director
National CyberWatch Center
maccdc@nationalcyerwatch.org

REGIONAL FINAL OVERVIEW

The MACCDC Regional Final is presented by Raytheon Intelligence & Space and run by the National CyberWatch Center (NCC), 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 are able to 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.

BLUE TEAMS

The following teams will be competing in the 2021 MACCDC Regional Finals:

- Capitol Technology University
- George Mason University
- Liberty University
- Millersville University
- Northern Virginia Community College
- Old Dominion University
- University of Maryland Baltimore County
- University of Pittsburgh

The winning team will represent the Mid-Atlantic Region in the National CCDC, April 23–25 (dates subject to change). NOTE: The second-place team from the MACCDC will compete in a Wild Card round on April 7. The winner of that round will advance to the National CCDC as well.

SCHEDULE

Friday, April 2: Day 1 Competition (all times EDT)

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

Saturday, April 3: Day 2 Competition (all times EDT)

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

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 subsequent to 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.
- **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.
- **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.

SCENARIO

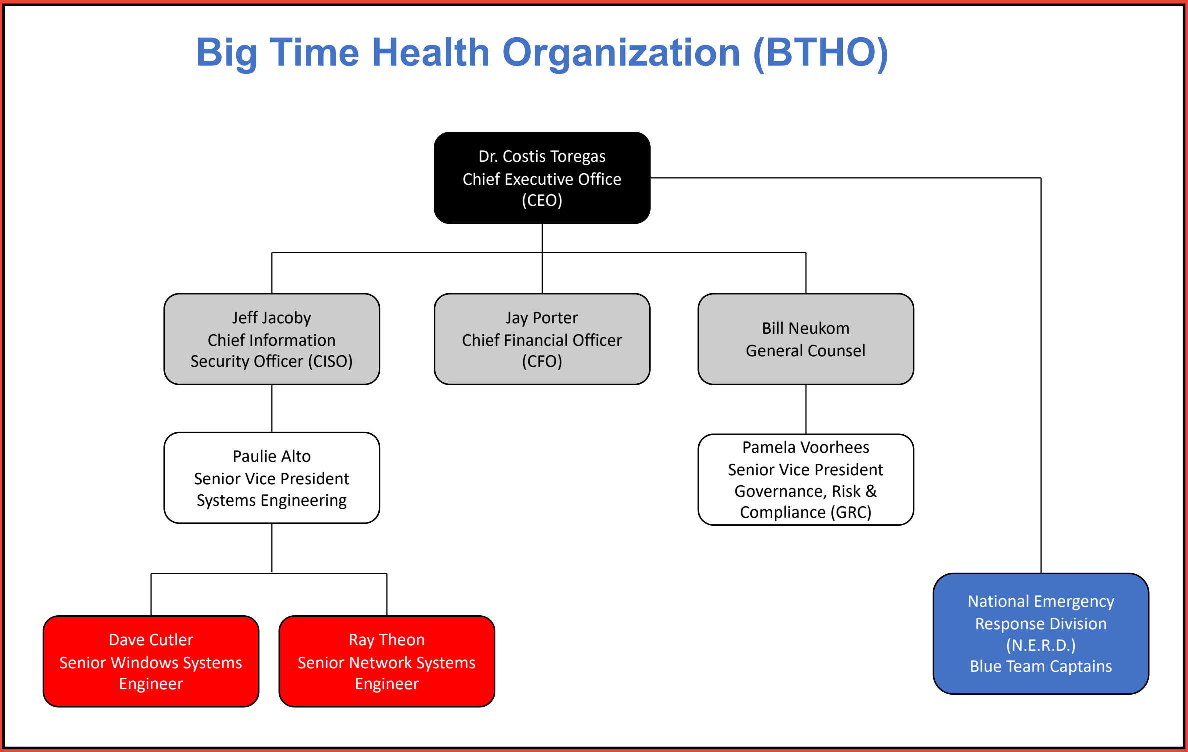

Big Time Health Organization (BTHO)
Dr. Costis Toregas Chief Executive Office (CEO)
Jeff Jacoby Chief Information Security Officer (CISO)
Jay Porter Chief Financial Officer (CFO)
Bill Neukom General Counsel
Paulie Alto Senior Vice President Systems Engineering
Pamela Voorhees Senior Vice President Governance, Risk & Compliance (GRC)
Dave Cutler Senior Windows Systems Engineer
Ray Theon Senior Network Systems Engineer
National Emergency Response Division (N.E.R.D.) Blue Team Captains

Fig. 1: BTHO Organization Chart

PANDEMIC

Over the past 16 years, the MACCDC has innovated, developed, and sought to create an original experience for not only the student teams, but all participants. Introducing themes that imitate real life adds a dimension of realism and funfree and secure elections, natural disasters, even Nerf gun fights. While 2020 was fraught with many challenges that were considered for the 2021 MACCDC scenario, the COVID-19 pandemic seemed the obvious choice.

The National Emergency Response Division (N.E.R.D.) is a data-science-focused group within the Big Time Health Organization (BTHO), a multinational entity headquartered in Bethesda, Maryland. N.E.R.D. employees have been exceptionally busy dealing with the pandemic. As such, they have had to shift to work from home as well as expand the number of employees to support the inordinate amounts of data flooding each of its eight geographic locations throughout the United States. Protecting the integrity of the data is critical, but when the data affect the delivery of health services to the public, the job of N.E.R.D. becomes even more mission critical.

The student teams will stand on the front lines of technology, alongside various health-care providers. The main task at hand will be ensuring that pandemic-related data from state departments of health are accurate and delivered quickly. Information on outbreak locations, promising interventions, efficacy of testing, mortality rates, and other related statistics are critical so that physicians, public health officials, and government entities can make informed decisions about resource allocations. Loss or inaccurate information can lead to tragic consequences. Vigilance is a must – be smart, be strong, be safe.

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. 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 of competition rules and their commitment to abide by those rules.

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.

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, quarter, or trimester.

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 Competition 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 Competition Director of the first CCDC event they participate in during a given CCDC competition season. Rosters must be submitted at least 2 weeks prior to the start of that event. 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 members chosen from the submitted roster.

c. Each competition team may have no more than two graduate students as team members.

d. If a member of a competition team advancing to a qualifying, state, regional, or national competition is unable to attend that competition, their team may substitute another student from the roster 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.

i. Team representatives must petition the Competition Director in writing for permission to make any changes to the competition team.

ii. The Competition Director must approve any substitutions or additions prior to those actions occurring.

f. 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.

g. 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 other 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.

h. An institution is only allowed to compete one team in any CCDC event or season.

i. A CCDC team may only compete in one region during any given CCDC season.

j. Exhibition (or unofficial) 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 completion of that event.

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 and coaches may not participate on the Red Team, Gold Team, White Team, or any such-related team at any CCDC event.

4. Competition Conduct

a. Throughout the competition, Gold and White Team members will occasionally need access to a team's system(s) for scoring, troubleshooting, etc. Teams must immediately allow Gold and White 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 a Gold or White Team member.

c. Teams may not modify the hardware configurations of competition systems. Teams must not open the case of any server, printer, computer, 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 Gold or White Team.

d. Teams may not remove any item from the competition area unless specifically authorized to do so by Gold 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 immediate 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 their own printed reference materials to the competition.

h. Team representatives, 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. 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 as to whether specific actions can be considered offensive in nature, team members should contact the Gold Team before performing those actions.

k. Teams are allowed to use active response mechanisms (e.g., Transmission Control Protocol resets) when responding to suspicious or 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, Intrusion Detection System, Intrusion Prevention System, 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 their team affiliation at all times during competition hours.

m. Only Gold 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 choose to are permitted.

b. Teams may not use any external, private electronic staging area or File Transfer Protocol (FTP) site for patches, software, etc., during the competition. Teams are not allowed to access private Internet-accessible libraries, FTP sites, websites, network storage, email accounts, or shared drives during the competition. The use of external collaboration and storage environments (e.g., Google Docs/Drive) is prohibited unless read access is given to the Regional Director or Competition Director prior to the start of the competition. All Internet resources used during the competition must be freely available to all other teams. 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. 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 AIM, chat, email or any other public or non-public services including sites such as Facebook. For the purposes of this competition, inappropriate content includes pornography or explicit materials, pirated files, sites containing key generators, and pirated software. If there are any questions or concerns during the competition as to whether specific materials are unauthorized, team members should contact the Gold and/or 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, that 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 the 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.

6. Permitted Materials

a. No memory sticks, flash drives, removable drives, CD-ROMs, electronic media, or other similar electronic devices are allowed in the room during the competition unless specifically authorized by the Gold 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, cell phone, smartphone, or wireless device into the competition area unless specifically authorized by the Gold 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.

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

7. Professional Conduct

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

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 and drug free. Alcohol and drug use are not permitted at any time during competition hours or during any related CCDC event (e.g., Job Fair).

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 Team 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 Team or asked to leave the competition entirely by the Competition Director or Gold Team.

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 White Team 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 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 and 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 (if applicable), usage of recovery services (e.g., reverting a virtual machine to a known good state), and successful penetrations by the Red Team.

b. Scores will be maintained by the Gold Team 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 team action that interrupts the scoring system is exclusively the responsibility of that team and will result in a lower score. Any team member who modifies a competition system or system component, with or without intent, 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 Internet Protocol (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. 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 ensure compliance with all event rules.

ii. Provide direction and clarification to the team as to rules and requirements.

iii. Establish communication with the Gold and White Teams 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. Ensure the Team Captain has communicated to the Gold or White Team 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 the Gold Team.

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 the Gold or White Team.

xii. Provide feedback to students subsequent to the completion of the CCDC event.

b. Each Coach or Team Captain must send the name, phone number, and email address of their Remote Site Judge to the MACCDC Regional Director by March 31.

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.

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. 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)

5. 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 free reverts total for the entire event, per team. Each additional request for a VM snapshot revert will carry a 20% point penalty in the total service score for the event.

6. C-Level Executive Meetings: Each Team Captain will meet face-to-face with the CEO, CFO, and CISO of the BTHO (see the schedule below). During the initial meeting on Day 1 (10 minutes, timed), these executives will expect to be briefed on the current 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: Capitol Technology University
- 11:15am: George Mason University
- 11:30am: Liberty University
- 11:45am: Millersville University
- 12:00pm: Northern Virginia Community College
- 12:15pm: Old Dominion University
- 12:30pm: University of Maryland Baltimore County
- 12:45pm: University of Pittsburgh

During the second meeting on Day 2 (10 minutes, timed), each Team Captain will meet again with the CEO, CFO, and CISO 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 – Level Executive Meeting Schedule:

- 11:00am: Capitol Technology University
- 11:15am: George Mason University
- 11:30am: Liberty University
- 11:45am: Millersville University
- 12:00pm: Northern Virginia Community College
- 12:15pm: Old Dominion University
- 12:30pm: University of Maryland Baltimore County
- 12:45pm: University of Pittsburgh

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

7. Incident Response: All Blue Teams must submit at least four Incident Response forms and open two cases with the Incident Response officials in attendance (they are part of the White Team). Incident Response forms will be provided. Instructions for submitting these forms will be provided during the initial team briefing on Day 1. Incident Response forms will be scored based on coherence and technical accuracy and depth. A thorough 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.

Calculating Scores:

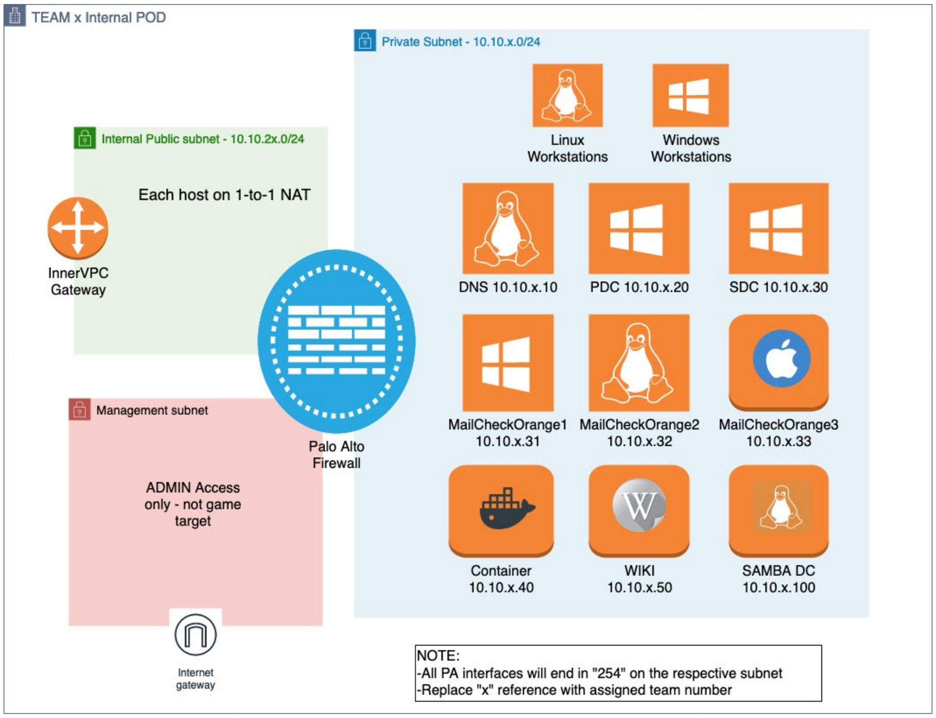
- All Blue Teams start with zero points.
- Raw scores are used for the scoring metrics, excluding the Red Team (which uses an ordinal scale, see next).
- Blue Teams are ranked using an ordinal scale, which is a measurement scale that assigns values to objects based on their ranking with respect to one 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 of the scoring metrics.
- The ordinal scores from all of the scoring metrics 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.

FUNCTIONAL SERVICES

Certain services are expected to be operational at all times. 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:

IP	Type	Port	Description
10.10.X.254	HTTP(S)	443	Palo Alto Administrative Interface
10.10.X.10	DNS	53	DNS Server – BIND9
10.10.X.10	SSH	22	DNS Server – Administrative Access
10.10.X.20	SMB	445	Primary Domain Controller – Administrative Access
10.10.X.20	KERB	88	Primary Domain Controller – Kerberos Authentication
10.10.X.30	RDP	3389	Secondary Domain Controller – Remote Desktop
10.10.X.30	RR	445	Secondary Domain Controller – Remote Registry
10.10.X.40	DOCKER	2375	Container Server – Docker
10.10.X.40	SSH	22	Container Server – Administrative Access
10.10.X.50	HTTP	80	Internal Wiki – DokuWiki
10.10.X.50	SSH	22	Internal Wiki – Administrative Access
10.10.X.100	SMB	445	Backup Domain Controller – Administrative Shares
10.20.X.10	HTTP(S)	443	GIT Server – Internal GitHub Web Service
10.20.X.10	SSH	22	GIT Server – Git push/pull over SSH
10.20.X.20	HTTP	80	Jenkins Server – Build Server
10.20.X.30	HTTP	80	Tomcat Server – Production Site
10.20.X.30	SSH	22	Tomcat Server – Administrative Access
X.10, X,20, X,30	CI	22	White CI Check – End-to-End build of product
	80, 80		This check required GIT, Jenkins, and Tomcat
10.30.X.10	RDP	3389	Jump Server – Remote Desktop
10.30.X.20	FTP	21	Secrets Vault – File Transfer Protocol
10.30.X.20	SMB	445	Secrets Vault – Samba File Share

COMPETITION TOPOLOGIES



NOTE:
-All PA interfaces will end in "254" on the respective subnet
-Replace "x" reference with assigned team number

Fig. 3: Team's Internal Network

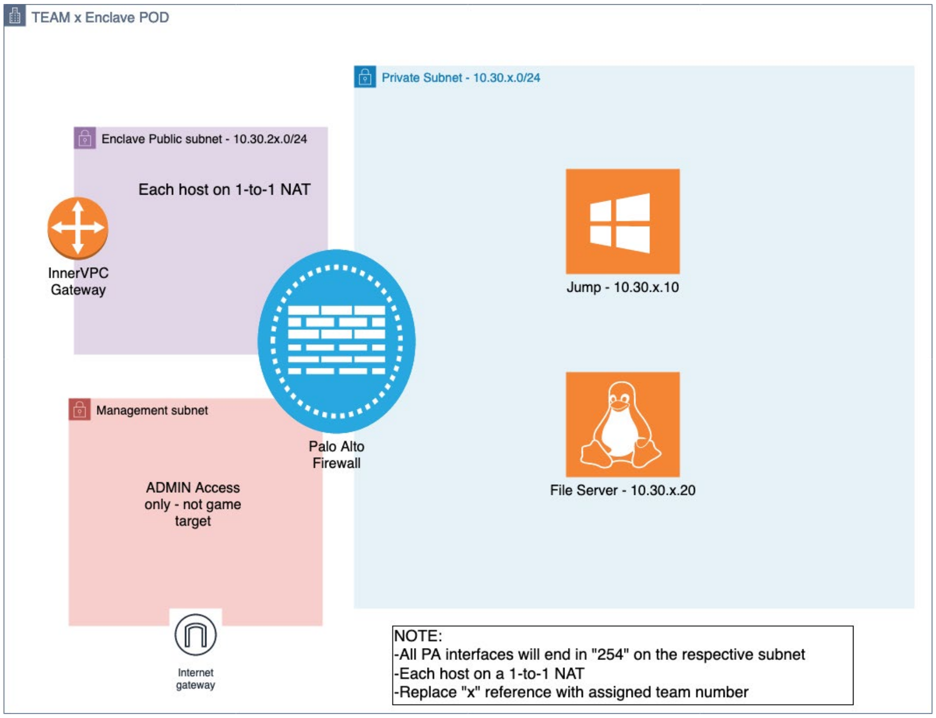

TEAM x Enclave POD
Private Subnet - 10.30.x.0/24
Enclave Public subnet - 10.30.2x.0/24
Each host on 1-to-1 NAT
InnerVPC Gateway
Jump - 10.30.x.10
Palo Alto Firewall
Management subnet
ADMIN Access only - not game target
File Server - 10.30.x.20
Internet gateway
NOTE:
-All PA interfaces will end in "254" on the respective subnet
-Each host on a 1-to-1 NAT
-Replace "x" reference with assigned team number

Fig. 4: Team's Enclave Network

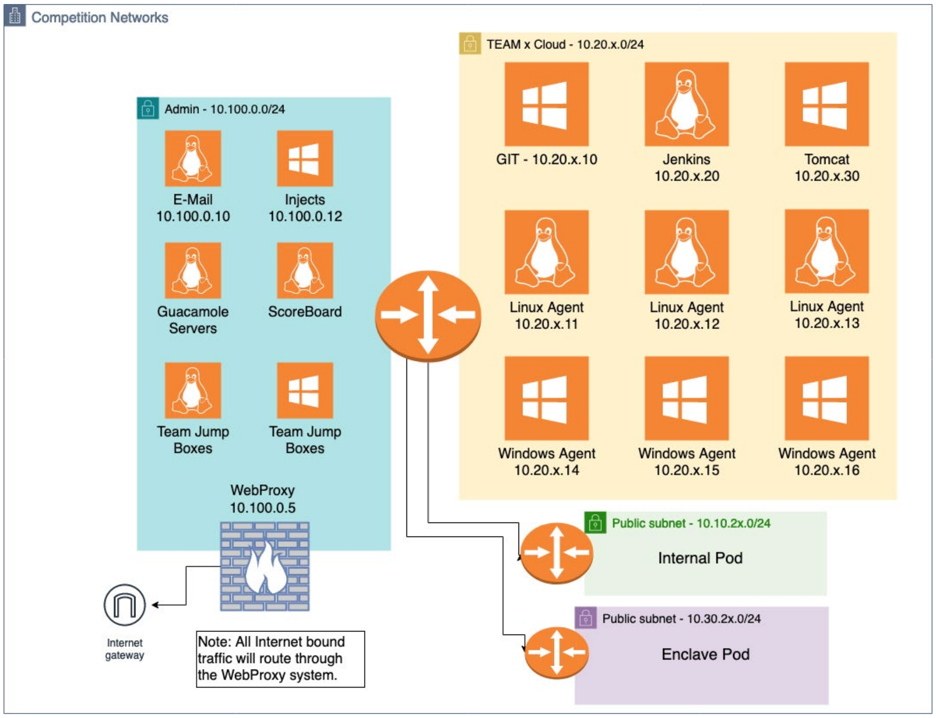


Fig. 5: Competition Networks

SYSTEMS

1. Each team will start the competition with identically configured systems.

2. Teams may not add or remove any computer, printer, or networking device from the designated competition area (where applicable).

3. Teams should not assume any competition system is properly functioning or secure.

4. Throughout the competition, Gold and White Team members will occasionally need access to a team's systems for scoring, troubleshooting, etc. Teams must allow Gold and White Team member access when requested.

5. 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.

6. 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. Likewise, teams are not permitted to change the internal addressing or virtual local area network scheme of the competition network unless directed to do so by an inject.

7. Teams may re-task servers, moving a service from one server to another, provided the outside "public" IP address of the service remains the same. It is the responsibility of the team to understand all the particulars of scoring a service when doing so.

8. Teams are not permitted to alter the system names or IP address of their assigned systems unless directed by an inject; this may affect the results of the scoring mechanism.

9. Systems designated as user workstations within the competition network are to be treated solely as user workstations and may not be re-tasked for any other purpose by teams.

10. Teams may not modify the hardware configurations of workstations used to access the competition network (where appropriate).

11. Servers and networking equipment may be re-tasked or reconfigured, as needed.

12. Red Team activity will be active throughout the event. At no time will the Red Team have access outside the Cyber Stadium perimeter.

13. Each Blue Team network will be monitored by a scoring system operating within the remote network. An indication of services, as viewed by the indigenous scoring engine, will be made available to each Blue Team via the Scoreboard range.

14. 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 Lead.

SPONSORS

Presented by: Raytheon Intelligence & Space

Produced by: NATIONAL CYBERWATCH CENTER

Gold: paloalto® NETWORKS

Silver: SEALING TECH

Supporters: APL JOHNS HOPKINS APPLIED PHYSICS LABORATORY

BOGDAN COMPUTER SERVICES

cobaltstrike

CROWDSTRIKE