Mid-Atlantic Collegiate
Cyber Defense Competition

2023 Regional Round
Blue Team Packet

"REDACTED" pre-competition packet

Presented by

Raytheon
Intelligence & Space

Run by

MetaCTF

NATIONAL
CYBERWATCH
CENTER

Mid-Atlantic Collegiate
Cyber Defense Competition

Table of Contents

Mid-Atlantic Collegiate
Cyber Defense Competition

Overview

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" (from 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.

Competition Goals

1. To promote fair and equitable standards for cyber defense and technology-based competitions that can be recognized by industry.
2. To evaluate the defensive and responsive skills of each team under exact hardware, software application, and operating system configurations using a joint academic and industry rating scale.
3. To demonstrate the effectiveness of each participating institution’s academic security program.
4. To be executed by a preponderance of industry professionals.
5. To have industry recognition, participation, and acceptance of each competition.
6. To rate the effectiveness of each competition against a predefined standard of competition rules.

7. To provide a cooperative and competitive atmosphere among industry partners and academia in cyber defense education.
8. To provide recognition for participating teams.
9. To increase public awareness of academic and industry efforts in cyber defense education.

Competition Teams

Throughout this document, the following terms will be used:

- **Gold/Operations Team**: Competition officials who organize, run, and manage the competition. Responsibilities include, but are not limited to:
    - Administer, staff, and orchestrate the event.
    - Manage scoring elements and determine final standings.
    - Has the authority to dismiss any team, team member, or visitor for violation of competition rules, inappropriate, and/or unprofessional conduct
    - Make provision for awards and recognition.
- **Black Team**: Competition support members who design and implement the competition infrastructure, provide technical support, and provide overall administrative support to the competition.
- **White Team**: Competition officials who evaluate team performance, ensure rule compliance, deliver and score injects, and volunteer in various other positions during the competition.
- **Orange Team**: competition officials who serve as the end users of Blue Team systems and evaluate availability of services.
- **Blue Teams**: The student teams 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 Gold/White Teams.
    - **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

MACCDC Overview

The MACCDC is one of the 9 regional CCDC events in the United States. Now in its 18th year, our region represents four-year universities and community colleges from Delaware, the District of Columbia, Maryland, New Jersey, North Carolina, Pennsylvania, Virginia, and West Virginia. Since its inception, over 3,500 students have participated in the MACCDC.

The MACCDC is one of the 9 regional CCDC events in the United States. Now in its 18th year, our region represents four-year universities and community colleges from Delaware, the District of Columbia, Maryland, New Jersey, North Carolina, Pennsylvania, Virginia, and West Virginia. Since its inception, over 3,500 students have participated in the MACCDC.

This competition consists of both a qualifying round and a regional final round. The virtual qualifying round took place on February 4th, and the top 8 teams from 26 participating universities advanced to the in-person regional competition at Prince George's Community College on March 31st - April 1st. The winner of the regional competition will advance to the national round.

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 who must "inherit-and-defend" an IT infrastructure. The teams are expected to manage the systems, keep them operational, and prevent unauthorized access. Each team starts the competition with a set of identically configured systems. This is not just a technical competition, but also one built upon the foundation of business operations, policies, and procedures. A technical success that adversely impacts the business operation will result in a lower score as will a business success which results in security weaknesses.

Student teams are scored on their ability to detect and respond to outside threats, while maintaining availability of existing network and application services, responding to business requests, also known as injects, and balancing security against varying business needs. For more details, see the Scoring section below.

Mid-Atlantic Collegiate
Cyber Defense Competition

Regional Round

Schedule

Friday, March 31st

7:30am - 8:20am	Blue Team Check-In
8:30am - 8:50am	Morning Briefing (Proscenium)
9:00am - 5:00pm	Competition Day 1 (Black Box Theater)
11:00am - 1:00pm	C-level Meetings
1:00pm - 2:00pm	Lunch Break, Competition Paused
5:15pm - 6:00pm	Day 1 Debrief (Black Box Theater)
6:00pm – 6:30pm	Sponsor Introductions (Black Box Theater)
6:30pm - 9:30pm	Career Fair and Networking Event (Atrium and Conference Rooms)

Saturday, April 1st

8:30am - 8:50am	Morning Briefing (Proscenium)
9:00am - 4:00pm	Competition Day 2 (Black Box Theater)
11:00am - 1:00pm	C-level Meetings
1:00pm - 2:00pm	Lunch Break, Competition Paused
4:00pm – 5:00pm	Competition Breakdown
5:30pm - 6:30pm	Competition Debrief and Awards (Proscenium)

Teams

From the 26 schools who compete in the 2023 qualifying round, the following 7 schools have qualified and are able to compete in the regional round.

- George Mason University
- Liberty University
- Messiah University
- The Pennsylvania State University
- Rutgers University
- University of Virginia
- Virginia Tech

Old Dominion University had qualified to compete in the regional competition, but they have been unable to field a team.

Mid-Atlantic Collegiate
Cyber Defense Competition

CCDC Rules

Mid-Atlantic CCDC follows the competition rules established by the National CCDC (http://nationalccdc.org/index.php/competition/competitors/rules). They provide structure for the makeup of student teams, permitted actions during competition play, 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. 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. Access to the competition stadium environment (both virtual and/or in-person) implies their acknowledgement of competition rules and their commitment to abide by them.

Regionals Scoring

Scoring is based on keeping required services up, controlling/preventing unauthorized access, and completing business tasks (injects) that will be provided throughout the competition.

Scores are maintained by the Gold/Operations Team, working in conjunction with the Black, Red, Orange, and White Team leads. Individual tracking of services may be available to respective teams during the competition. Blue Team members should use available the available scoring engine and manual testing to assess the integrity of their networks and systems. Blue Team members should refrain from making direct requests to the Black or White Teams for routine service verification.

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. **Service Level Agreements (SLAs)**. There will be no SLA penalties during the regional round.
    b. **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) only for the AWS services. No reverts will be available for services running on the on-prem systems. Teams are allowed one (1) free revert 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. Teams will also be allowed to request a reset of their Cisco FTDs between Day 1 and Day 2.

c. **Black Team Agent (BTA).** Every host on the competition network will be running a special Black Team Agent service that will be used to help score machine uptime, service uptime, and red team activity.
    i. The BTA needs to be able to reach the scoring server via HTTPS (port 443) at the IP address 10.250.250.11. BTA check-ins will be reported on the scoreboard.
    ii. If the BTA is disabled or blocked from reaching the scoring server, severe point penalties will be applied.
    iii. The BTA will be running as the root or Administrator user and installed as an auto-start service named `bta` on all platforms.
    iv. The Red Team has been instructed not to inject into or tamper with the BTA in any way.
    v. Any attempt by Blue Teams to tamper with, impersonate, or hinder communication of the BTA will result in heavy point penalties or disqualification.
    vi. The Blue Teams will be able to verify the status of the BTA on their machines in the Scoring Engine.
    vii. The BTA may perform additional checks on local network services such as SMB, HTTP, LDAP, and SSH. These additional checks will be made locally only (i.e. to localhost), so no additional ports need to be opened for the BTA for it to function properly. Any questions about the BTA should be asked before the competition starts.

d. **Electronic Badges.** TENTATIVE. This may not happen:
    i. Each team will have 8 electronic badges that represent shipping containers (regardless of actual team size). 7 will be for team members and 1 will be for the captain with capacities of 100 and 800 “items” respectively.
    ii. The badges will accumulate items every hour. Team members can unload those “items” onto the docking station and the team captain badge will load those items from the docking station
    iii. Every hour, team captains will go to the white team to unload the “items” for points.
    iv. The badges score will be worth 25% of your service score

2. **Injects**. Throughout the competition, Blue Teams will be presented with injects. An inject is any assigned task to be completed in the assigned amount of time. Inject types vary, and point totals are 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.
    a. Injects will be released automatically to all teams at the same time on the Scoring Engine platform that will also be used to score services. It is the team’s responsibility to periodically check the Scoring Engine for newly released injects.

b. Injects will be submitted on paper. Any inject submitted in the Scoring Engine will not be graded unless explicitly requested by the inject grading team. Teams will have to print the inject from the shared printers. Teams will be provided with flash drives to transfer files from their team's in-competition laptops to the laptops that have access to the printers. These flash drives cannot leave the competition area.
c. Since injects will be printed, please attempt to use a white background for your terminal/text editor/IDE screenshots.
d. Each inject must contain the team number and the inject number & title the inject is for.
e. 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. Different injects may have different point values.
f. No points will be awarded for the inject if the inject is submitted late.
g. Unless indicated otherwise, the Team Captain may assign injects to specific team members for completion.
h. Red Team (or Blue Team) activity can adversely affect a team's ability to complete injects. It is the Blue Teams' responsibility to maintain system availability. No extra time or point credit will be given for injects that are not completed because of inability to access a system.
i. You will not be able to re-submit injects unless notified by the white team.

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 (e.g., compromising a server, stealing data). All Red Team activities are meant to disrupt or misinform. At the conclusion of each competition day, the Red Team will rank each team from best to worst.
4. **Incident Response Reports.** 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.
5. **Executive Meetings.** Each Team Captain will meet face-to-face with various Hulk Bulk Shipping executives.
   During the initial meeting on Day 1, the Team Captains will be given action items to complete within a fixed time. Teams will then have 60 minutes to submit an initial version of those reports on paper, after which Team Captains will meet with the executives individually and present their reports. The executives may also ask 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.
During the meeting on Day 2, each Team Captain will meet again with various C-Level executives, deliver the final version of the report requested in the first Day 1 meeting, and provide updates on any changes that transpired.
Day 1:

- 9:45am: initial meeting (all captains present)
- 10:45am: initial report due
- 11:00am - 1:00pm: individual meetings with each of the team captains

Day 2:

- 11:00am - 1:00pm: individual meetings with each of the team captains

6. **Orange Team.** The Orange Team represents the end users and employees of Hulk Bulk Shipping. They will test services for functionality and data integrity every hour. The Orange Team will attempt to use the company services and communicate with the blue teams if they run into issues. Every hour, several of the team's services will be checked for uptime, functionality, and data integrity. If the Orange Team finds that a service is down, they will attempt to call the team to resolve the issue. Teams will receive 0 points for the check if the service was down and the team did not resolve their issue, 1 point if the service was down but the issue was resolved, and 2 points if the service was up.

Calculating Scores

- Raw scores are used for the above scoring metrics, excluding the Red Team.
- Blue Teams will be assigned a rank for each scoring metric using standard competition ranking, 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, and on. Same raw scores will have the same rank. For example, four teams with scores of 2000, 1750, 1750, and 1500, will be ranked 1, 2, 2, and 4 respectively. This process will be repeated for all the scoring metrics, excluding the Red Team.
- The ordinal scores from all 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 last 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, the team with the higher raw inject score will place better. If there's still a tie, the raw service score and then the Red Team ranking will be used as secondary and tertiary tie breakers respectively.

Mid-Atlantic Collegiate
Cyber Defense Competition

Scenario & Infrastructure

Hulk Bulk Shipping

Hulk Bulk Shipping is a leading online retail and distribution company. Operating globally, the company offers a wide range of products and services to customers around the world from many third-party sellers.

In addition to its e-commerce operations, "Hulk Bulk Shipping" also boasts an efficient and reliable delivery service. With a network of warehouses and fulfillment centers around the world, the company is able to get purchases to customers quickly and efficiently, no matter where they are located.

Due to a recent breach, the company underwent a major restructuring of its IT department, and a new IT team was brought in to replace the former team. The new IT team is tasked with securing and defending the company's network while also ensuring that business operations can continue smoothly.

Competition Topology

Each team will be responsible for managing and protecting several virtual machines and on-prem devices in their networks.

The X's in the IP addresses correspond to each team's randomly assigned team number.

Network Segment	Hostname	IP Address	Operating System
cloud	dropbox	10.250.20X.13	Ubuntu 18.04
cloud	blog	10.250.20X.39	Red Hat 8
cloud	intern	10.250.20X.42	Rocky 8
cloud	people	10.250.20X.55	Debian 10
cloud	customer	10.250.20X.88	Ubuntu 20
cloud	office	10.250.20X.114	Ubuntu 20
cloud	draw	10.250.20X.142	Rocky 8
cloud	inventory	10.250.20X.152	openSUSE 15
cloud	sso	10.250.20X.168	Windows Server 2016
cloud	packages	10.250.20X.182	Debian 10
cloud	code	10.250.20X.194	Ubuntu 18.04
cloud	collab	10.250.20X.211	Amazon Linux 2
cloud	hr	10.250.20X.234	Windows Server 2012 R2
core	corefw	10.250.X.254	Cisco ASA

core	siem	10.250.X.19	Fedora 34
core	cdc01	10.250.X.20	Windows Server 2016 Core
core	automate	10.250.X.37	Amazon Linux 2
core	edr	10.250.X.61	Amazon Linux 2
core	coredb	10.250.X.100	Windows Server 2019
core	connect	10.250.X.129	Palo Alto PAN OS
core	backups	10.250.X.140	Windows Server 2012 R2
core	leeroy	10.250.X.162	FreeBSD 12
core	keys	10.250.X.176	Windows Server 2016
core	assets	10.250.X.230	CentOS 7
hq	virtual	172.2X.0.1	Proxmox
hq	wk1	172.2X.0.2	Gallium OS
hq	wk2	172.2X.0.3	Gallium OS
hq	wk3	172.2X.0.4	Gallium OS
hq	wk4	172.2X.0.5	Gallium OS
hq	wk5	172.2X.0.6	Gallium OS
hq	wk6	172.2X.0.7	Gallium OS
hq	wk7	172.2X.0.8	Windows 10
hq	wk8	172.2X.0.9	Windows 10
hq	hqdc01	172.2X.0.10	(virtual) Windows Server 2016
hq	cert	172.2X.0.44	(virtual) Windows Server 2019
hq	storage	172.2X.0.93	(virtual) Windows Server 2012 R2
hq	chat	172.2X.0.117	(virtual) Ubuntu 20
hq	password	172.2X.0.139	(virtual) Rocky 8
hq	git	172.2X.0.173	(virtual) Rocky 8
hq	legacy	172.2X.0.202	(virtual) Windows XP
hq	container	172.2X.0.227	(virtual) Alpine
hq	fun	172.2X.0.234	(virtual) Alpine
hq	ap	172.2X.0.250	Dlink DAP-1360C1
hq	camera	172.2X.0.251	VStarcam C7824WIP
hq	call	172.2X.0.252	Cisco 7900 VOIP
hq	hqfw	172.2X.0.254	(virtual) Cisco Firepower

Scored Services

The in-scope virtual machines may contain one or more scored services that will be periodically checked by the scoring service. In addition to being up and accepting connections, the services must be functional and serve the intended business purpose.

THIS WILL BE PROVIDED IN PERSON.

Credentials

Blue Teams will be able to log into the virtual machines and applications using the following default credentials. Pick the username specific to the operating system.

THIS WILL BE PROVIDED IN PERSON.

Scored Service Descriptions

Below you will find the descriptions of each of the scored service types and an overview of how they will be scored. The scored services are subject to change. Refer to the Scoring Engine during the competition for most up-to-date information.

Some of the services below require authentication. The team will be able to manually update credentials for specified users in the Scoring Engine. This allows teams to rotate credentials without failing the checks in the scoring system.

HTTP - Hypertext Transfer Protocol
A request for a specific web page will be made and the response will be compared to the expected result. The returned page must match the expected content for points to be awarded.

HTTPS - Hypertext Transfer Protocol Secure
A request for a specific web page will be made over SSL. Similarly to HTTP, the response will compared to the expected value.

RDP - Remote Desktop
A specified user will attempt to log in via RDP to the service. If a desktop appears, the check will be successful.

SMB - Server Message Block
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.

DNS - Domain Name System

DNS lookups will be performed against the team's DNS server. Each successfully served request will be awarded points.

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 to the expected stored value.

PostgreSQL (Database)
Similar to the MySQL check, a connection to the database will be made with a specified user and a query will be run.

FTP - File Transfer Protocol
A connection to the server will be made with a specified user, a file will be retrieved, and its contents will be checked against an expected value.

SSH - Secure Shell
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.

LDAP - Lightweight Directory Access Protocol
An authenticated query to the Active Directory LDAP service will be performed.

WinRM - Windows Remote Management
A WinRM session will be created with specified credentials and a command will be executed.

Elasticsearch
A record will be inserted using the Elasticsearch HTTP API and a request will be made to verify that the newly created record exists.

NFS - Network File System
The scoring script will connect to the NFS service and attempt to write to a file. It will then attempt to log in again and see if the file exists.

Firewalls

Teams can filter inbound and outbound external traffic by port/protocol but not by IP addresses or IP ranges. For example, you can allowlist certain inbound ports for all source IPs, but you cannot create firewall rules to blocklist or allowlist specific IPs from accessing that port. There are no restrictions on filtering local traffic between your team's machines if it doesn't interfere with any services. The black team will not help troubleshoot.

The BTA server, which receives connections on port 443, is not an exception. This effectively means that you cannot block any egress traffic destined to port 443. For example, you cannot block all outbound traffic to port 443 and allowlist the BTA server IP. You are still allowed to block other outbound traffic by port/protocol.

The only exception is you may request to block certain IP addresses in your IR report. If the IR team believes you have sufficient evidence and gives you permission to block it, you may do so.

Internet Access

- Approved software requests will be available for download from the software center at the competition start. The software center will be accessible from both on-prem and cloud machines.
- Access to public internet in the competition environment, including most package/update repositories, will be blocked.
- You are welcome to bring in a reasonable amount of printed materials (nothing digital).
- You will have access to laptops and printers that you can use for browsing internet and downloading publicly available resources. These laptops will be shared with other teams, and they will be completely outside of the competition network. You are allowed to use these laptops to download other programs from the internet (as long as they are allowed by the National's rules), but you will not be allowed to download GitHub repositories.
- Each team will also be provided with a flash drive, which you must keep in the competition area at all times.

Regionals Logistics, Clarifications, and Additional Rules

1. Some competition machines may contain sensitive data or PII belonging to the fictitious company or its customers. This data may be necessary to complete service checks or injects, and a leak of this data by the Red Team may also negatively impact the team's Red Team Activity rank. Teams are not forbidden from moving this data to other in-scope devices, but it may impact their ability to pass some service checks or complete some injects.
2. Please refer to the Scoring section above for more information about the new Black Team Agent. Neither the Blue nor the Red Teams are allowed to tamper with this service in any way.
3. You are allowed to restart your virtual machines as many times as you want with no point penalties (except points lost by your critical services being down while the machine is rebooting). Refer to the Scoring section for penalties if you need to completely reset a VM to its original state.

Systems

1. Each team will start the competition with identically configured systems.
2. Teams should not assume any competition system is properly functioning, secure, or malware-free. As the incoming security team, you are expected to become familiar with the environment and assess its current security posture. You should also put in the effort to have high assurance that your company systems are not compromised.
3. 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.
4. Network traffic generators may be used by competition organizers 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. Teams are not permitted to alter the system names or IP address of their assigned systems unless directed by an inject or the Gold/Operations team; this may affect the results of the scoring mechanism.
6. The competition topology is subject to change.

Questions and Disputes

1. Team captains are encouraged to work with their White team 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 Regional Director as soon as possible. The Regional Director (in consultation with the Gold/Operations/White/Red teams) will be the final arbitrator for any protests or questions arising before, during, or after the competition and rulings by the competition officials are final.
2. 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.
3. 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

The top team will advance to the in-person National CCDC competition. The second place team will have a second chance to earn a spot at Nationals in the Wildcard round.

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.