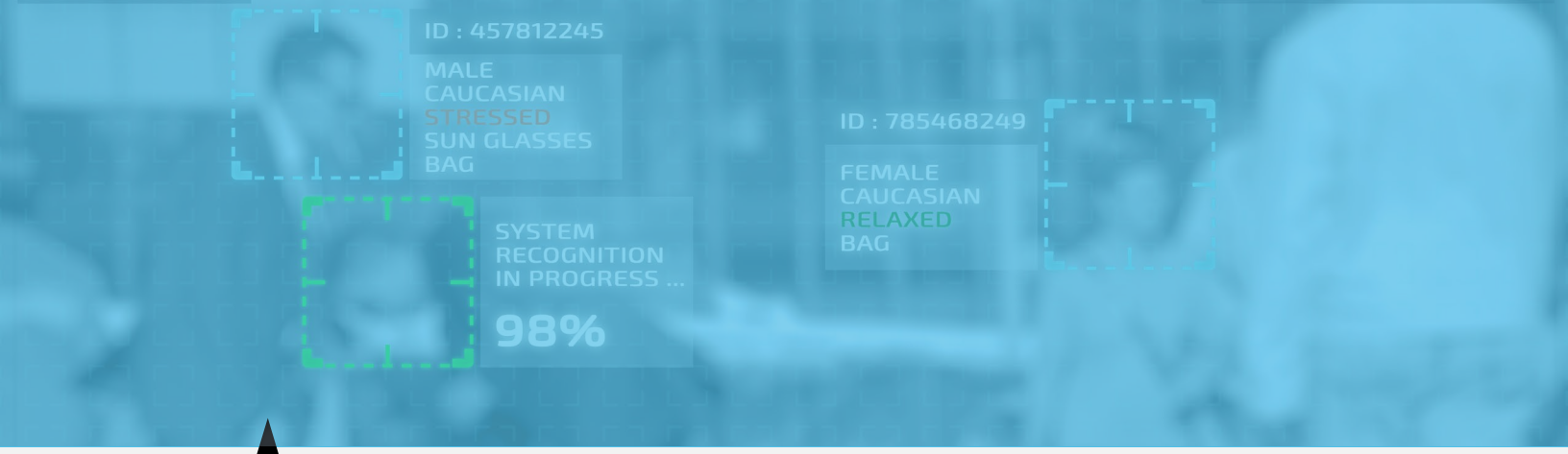

15th Annual

MID-ATLANTIC COLLEGIATE CYBER DEFENSE COMPETITION

Presented by

Raytheon

Mid-Atlantic Collegiate CYBER DEFENSE COMPETITION

2020

ARTIFICIAL INTELLIGENCE

NATIONAL CYBERWATCH CENTER

WELCOME

From March 24–26, 2006, five teams—Anne Arundel Community College, Community College of Baltimore County, George Mason University, Millersville University, and Towson University—gathered at the Burle Business Park in Lancaster, PA, for the first MACCDC.

The defending student Blue Teams assumed responsibility of the Globex IT infrastructure, a fictitious IT services/product reseller. By today's standards, the infrastructure was simple: each school defended a mere seven assets, including a router, a firewall, servers, and an IP surveillance camera. Four Red Team members ("hackers") attacked and disrupted the students' infrastructure. Scoring was accomplished using a custom Perl script that checked network and service availability and integrity. At the end of the three-day competition, Millersville University won, representing the Mid-Atlantic region at the National CCDC, April 21–23, 2006, and placing second overall nationally.

Throughout the years, the MACCDC has been one of the premier events of its type in the world. The *special sauce*, if you will, has always been a combination of amazing talent who plan and run the event (Tim Rosenberg, Dwight Hobbs, Lewis Lightner, Michael Dougherty, Larry Pesce, Paul Asadoorian, John Strand, Rob Fuller, Michael LaSalvia, Charlie Frick, John Sener, Costis Toregas…the list goes on); strong support and leadership from the National CCDC crew (Dr. Greg White, Dwyane Williams, Kevin Archer); dedicated faculty/coaches (Dr. Mike O'Leary, Todd Echterling); tremendous support from the Johns Hopkins University Applied Physics Laboratory; the latest technologies du jour (IPv4/v6 dual stack systems, SCADA, smart meters, cellular); fun and timely scenarios (health care IT, voting, natural disasters, transit, banking); a job fair and networking reception, linking employers with a supply of talented students looking for internships and full-time employment; and constant experimentation (a virtual qualifying round, broadcasting live play-by-play, modified Nerf guns, Red Teamers getting arrested for breaking the law).

What a journey from five teams and 31 participants in 2006 to over 3,200 full-time undergraduate and graduate-degree-seeking students, representing four-year universities and community colleges from Delaware, the District of Columbia, Maryland, New Jersey, North Carolina, Pennsylvania, Virginia, and West Virginia having competed in the MACCDC. Not to mention, the past three National CCDC Champions have come from the Mid-Atlantic region: the University of Maryland, Baltimore County (UMBC) in 2017 and the University of Virginia in 2018 and 2019.

As you can see, the MACCDC is more than a competition; it's culminated into what we call *event-anchored learning*, which is the use of an event to support, or "anchor," the learning experience. Why is it important? It engages participants, attracts stakeholders, adds value to the entire process, and supports all sorts of networking, capacity building, and program improvement activities.

Thank you to all of the individuals and organizations that have contributed to the success of this event over the years. Here's to 15 more.

Best regards,

Casey W. O'Brien
MACCDC Regional Director
National CyberWatch Center

ABOUT THE NATIONAL CYBERWATCH CENTER

The National CyberWatch Center (NCC) is a cybersecurity education and research consortium headquartered at Prince George's Community College in Maryland. NCC continues to be the go-to organization for innovative, scalable, and cost-effective information security education/training partnerships and solutions.

NCC has organized and run the MACCDC for the past 15 years. Additional programs and services include the following:

- Community College Cyber Summit (3CS)
- Cloud-based lab solution
- Curriculum offerings
- *Cybersecurity Skills Journal: Practice & Research*
- Innovations in Cybersecurity Education awards & recognition program
- Membership packages for academic institutions, individuals, and corporations
- National Cybersecurity Student Association
- Publications via its digital press
- Webcast series

For more information, visit https://www.nationalcyberwatch.org.

NATIONAL CYBERWATCH CENTER

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*, by Ron Dodge, Lance J. Hoffman, Daniel Ragsdale, and Tim Rosenberg, 2004)

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 of, participation at, 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/government partners and academia in the area of cyber defense education
8. To provide recognition for participating teams
9. To increase public awareness of academic, government, and industry efforts in the area of cyber defense education

TERMINOLOGY

Operations Team/Gold Team: competition officials who organize, run, and manage the competition

White **Team:** competition officials who observe team performance in their competition area and evaluate team performance and rule compliance

Red Team: penetration-testing professionals simulating external hackers attempting to gain unauthorized access to competition teams' systems

Black Team: competition support members who provide both technical and administrative support to the competition

Orange Team: competition officials who serve as end users of Blue Team systems and evaluate availability of services

Blue Teams: college and university 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 Representative: a faculty or staff representative of the Blue Team host college or university responsible for serving as a liaison between competition officials and the Blue Team's institution

2020 REGIONAL FINAL TEAMS

George Mason University

James Madison University

Liberty University

Marshall

PennState

UMBC

University of Maryland

University of Virginia

2020 QUALIFYING ROUND PARTICIPATING SCHOOLS

1. Bloomsburg University of Pennsylvania, Pennsylvania
2. Capitol Technology University, Maryland
3. Community College of Baltimore County, Maryland
4. Drexel University, Pennsylvania
5. East Carolina University, North Carolina
6. Frederick Community College, Maryland
7. George Mason University, Virginia
8. James Madison University, Virginia
9. Liberty University, Virginia
10. Marshall University, West Virginia
11. Millersville University, Pennsylvania
12. Northern Virginia Community College (Team 1), Virginia
13. Northern Virginia Community College (Team 2), Virginia
14. Pennsylvania State University, Pennsylvania
15. Polytechnic University of Puerto Rico, Puerto Rico
16. Saint Vincent College, Pennsylvania
17. Towson University, Maryland
18. University of Maryland, Baltimore County (Team 1), Maryland
19. University of Maryland, Baltimore County (Team 2), Maryland
20. University of Maryland, College Park, Maryland
21. University of Maryland Global Campus, Maryland
22. University of Virginia (Team 1), Virginia
23. University of Virginia (Team 2), Virginia
24. University of Virginia College at Wise, Virginia
25. Virginia Commonwealth University, Virginia
26. West Virginia University, West Virginia
27. Wilmington University, Delaware

SCENARIO

ARTIFICIAL INTELLIGENCE

Each year, the MACCDC develops a new exercise scenario and implements cutting-edge technologies that mimic those in the real world. This year's scenario involves student teams working for the Artificially Intelligent Institute (AII), pronounced *eye*.

AII is a multinational corporation with offices in the Mid-Atlantic region. As a leading provider of advanced AI surveillance tools to intelligence and law enforcement agencies, as well as private-sector organizations, the main business driver of AII is to show how new surveillance capabilities are transforming governments' and organizations' monitoring capabilities.

As part of their duties, Blue Teams are expected to defend their systems against aggressors. Early intelligence reports suggest that rogue Hackistanian antagonists are interested in stealing AII's intellectual property, source code, and customer database. Hackers contracted by and working directly for the country of Hackistan are also interested in disrupting IoT (Internet of Things) devices on premises at the various AII regional offices.

2020 SCHEDULE

Thursday, April 2

12:00 p.m. – 1:00 p.m.	Welcome and Sponsors' Briefings to Teams	Zoom
1:00 p.m. – 3:30 p.m.	Job Fair	Virtual Breakout Rooms

Friday, April 3

7:30 a.m. – 8:30 a.m.	Blue Team Check-In	Zoom
8:30 a.m. – 8:50 a.m.	Opening Competition Briefing	Zoom
9:00 a.m. – 5:00 p.m.	Day 1 Competition	Virtual Stadium
11:00 a.m. – 1:00 p.m.	CEO Meetings	Zoom
5:00 p.m.	Day 1 Competition Ends	
5:30 p.m.	Day 1 Debrief	Zoom

Saturday, April 4

7:30 a.m. – 8:30 a.m.	Blue Team Check-In	Zoom
8:30 a.m. – 8:50 a.m.	Morning Briefing	Zoom
9:00 a.m. – 5:00 p.m.	Day 2 Competition	Virtual Stadium
10:00 a.m. – 12:00 p.m.	CEO Meetings	Zoom
5:00 p.m.	Day 2 Competition Ends	
6:30 p.m. – 7:30 p.m.	Debrief and Awards Ceremony	Zoom

SCORING METRICS

1. **Services:** All scored services must remain up and available, with a high degree of integrity. All services are given predefined point values and will be checked periodically using service round checks. The actual number of service rounds will not be disclosed before 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 server, and attending meetings. Injects can be delivered through any number of methods, including electronically, on paper, and orally. Injects will be scored by a White Team member. If the inject is completed on time and to the standard required, the 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. Sample goals include compromising a server, stealing data, and modifying injects. All Red Team activities are meant to disrupt or misinform. Blue Teams are ranked based on their ability to defend their systems against the Red Team.

4. **CEO Reporting:** Each Team Captain will meet face-to-face with the CEO of All. During the initial meeting (10 minutes, timed), the CEO 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 will consider relevant for the CEO 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.

   During the second session (10 minutes, timed), each Team Captain will meet with the CEO and will have a chance to present written and verbal responses to what was covered in the first meeting and provide updates on any changes that transpired.

   Each team will be scored using the following metrics:

   - Oral presentation skills
   - 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 at least four Incident Response forms and open two cases with the Incident Response officials in attendance. Incident Response forms will be provided. Instruction for submitting Incident Response forms will be provided during the initial team briefing. Incident response forms will be scored based on coherence and technical accuracy/depth.

Raw scores are used for these scoring metrics. 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 functionality 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.

2020 SPONSORSHIP

To promote the competition's success and maintain the high quality associated with this program, we need to continue to maintain and grow a strong financial foundation. Sponsorships help defray institution costs and provide a meaningful way to engage with the design, execution, and evaluation of the event.

By taking an active role in sponsoring the MACCDC, organizations get the opportunity to get to know the best and brightest students specializing in information security from a variety of educational institutions. In addition, everyone attending will learn something from observing the students, listening to the Red Team debrief, and, in general, talking with the participants, organizers, and other observers.

Additional benefits to consider under special partnership arrangements include the following:

- Mentoring individuals or teams during preparation and after the event
- Monetary, software, and hardware contributions with tax benefits
- Lunch/dinner sponsorships
- Recognition on official marketing materials, in press releases, and on giveaways
- Participation in and recruitment of students at the Job Fair/Speed Networking Event
- Exclusive access to student resumes
- Participation on Red, White, and Orange Teams
- Test bed for new products and services

Producers

National CyberWatch Center

Johns Hopkins Applied Physics Laboratory

Named Sponsor (2020–2022)

Raytheon

Gold

paloalto Networks Cybersecurity Academy

Silver

780th Military Brigade

Air Force Civilian Service

SAIC

Supporters

Cobalt Strike — Advanced Threat Tactics for Penetration Testers

Bogdan Computer Services

SOCIAL MEDIA

Visit Us: https://maccdc.org

Follow Us: https://www.twitter.com/MidAtlanticCCDC, #15MACCDC and #15NCCDC

Like Us: https://www.facebook.com/MidAtlanticCCDC

Watch Us: https://www.youtube.com/user/Cyberwatchcenter

Look @ Us: https://www.flickr.com/photos/midatlanticccdc