



Women in CyberSecurity (WiCyS)

Global Nonprofit Organization



Ambareen Siraj
Celeste Matarazzo
Danielle Strimbu
Rosalie Olmsted

Betta Lyon Delsordo
Heather Holliday
Linxi Zhang
Suzanne Dove



**WiCyS 2026
Call For Presenters
Webinar**



Over
11K
members



WiCyS is a 501c3 nonprofit organization with global reach dedicated to bringing together *women in cybersecurity* from *academia, research and industry* to share *knowledge, experience, networking and mentoring.*



WiCyS Mission

Build a strong, robust cybersecurity workforce by facilitating...

RECRUITMENT

RETENTION

ADVANCEMENT for women in the field



Voice of WiCyS



Community



Recognition



Advocate



Growth



Leadership



Mentorship

WiCyS Timeline



WOMEN IN CYBERSECURITY INITIATIVES



PROGRAMS

Early Career
Mid Career
Senior Career



MEDIA

Newsletters
Speakers
Bureau
Speaking
Engagements



EVENTS

Annual
Conference
Regional
Affiliate Events
Virtual
Conference
Webinars



CAREER RESOURCES

Career Fairs
Career Growth
Hub
Conference
Scholarships &
Grants
JobBoard++
Research &
Resources
Resume
Reviews



COMMUNITY

11K+ Members
Affiliates
Board of
Directors
Committees
Mentorship
Mission
Support Team
Online Member
Platform
Senior Ally
Network
Student
Chapters

WOMEN IN CYBERSECURITY PROGRAMS



WiCyS Strategic Partners

TIER 1



TIER 2



TIER 3



Subscribe to the WiCyS Newsletter

[About ▾](#)[Join](#)[Initiatives ▾](#)[Programs ▾](#)[Support ▾](#)[Events ▾](#)[State of Inclusion](#)[Resources ▾](#)[Subscribe](#)[Login](#)

ADVANCING

Women in CyberSecurity

WiCyS is where the recruitment,
retention and advancement of women in
cybersecurity happens.

[JOIN US](#)[SUPPORT](#)

www.wicys.org



How it started



2014

How it's going

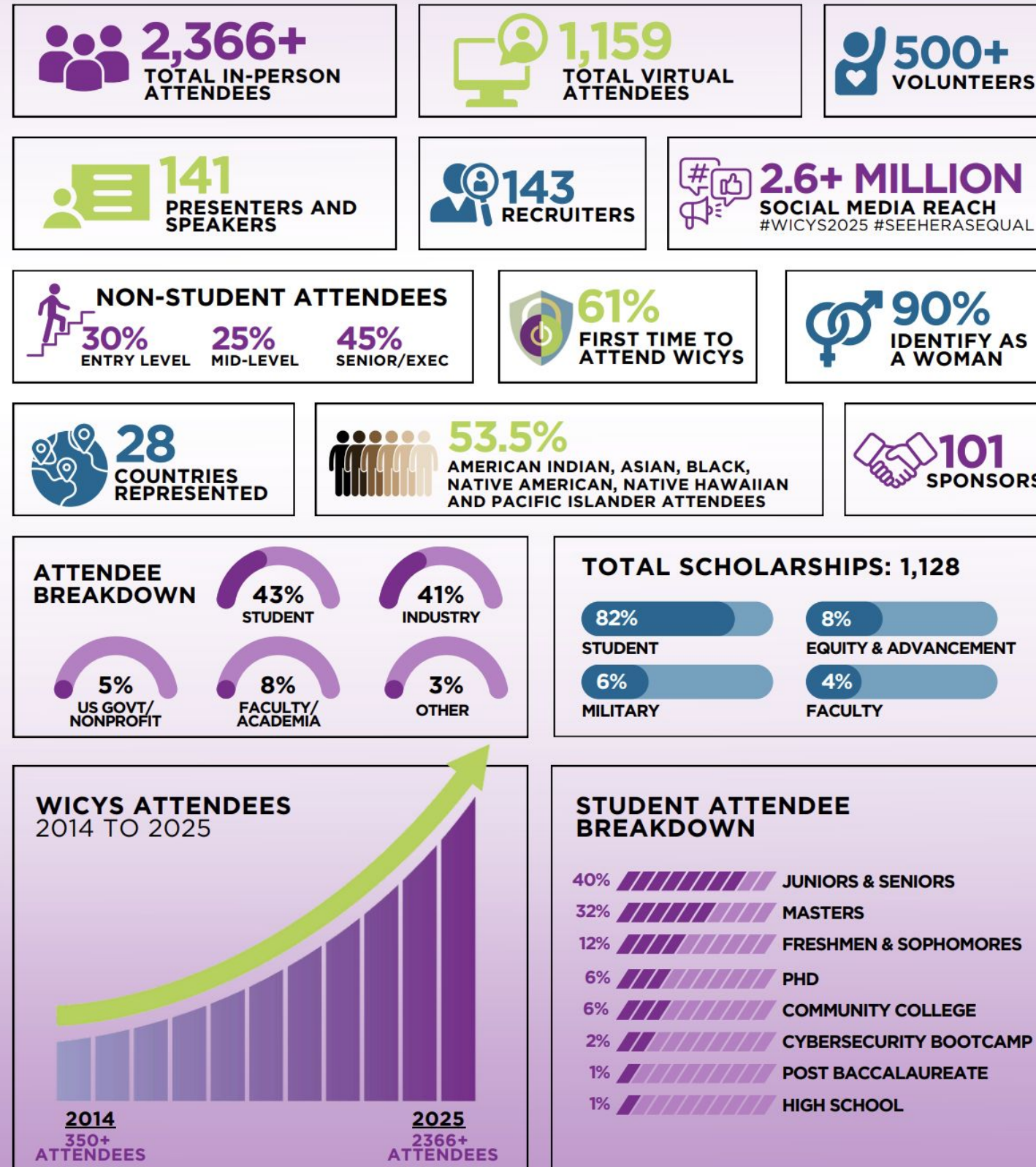


2025



RECRUIT, RETAIN and ADVANCE
Women in Cybersecurity

WICYS 2025 BY THE NUMBERS





WiCyS 2026 Conference

March 11 - 13, 2026

Gaylord National Harbor Resort and Convention Center
(Washington DC area)

WiCyS 2026 Virtual Conference

April 22 - 23, 2026



Program Committee

Conference Co-Chair (Program)

Dr. Ambareen Siraj, Founder WiCyS

Conference Co-Chair (Program Logistics)

Celeste Matarazzo, WiCyS

Program Coordinator

Danielle Strimbu, WiCyS

Program Co-Leads

- Dr. Amani Altarawneh
- Basma Basem
- Deborah Kariuki
- Elizabeth Rasnick
- Jillian Seabrook
- Dr. Junia Valente
- Miranda Skar
- Dr. Priyam Biswas
- Dr. Smriti Bhatt
- Xiao Zhang

**Supported by
A Large Group
of Reviewers!!**

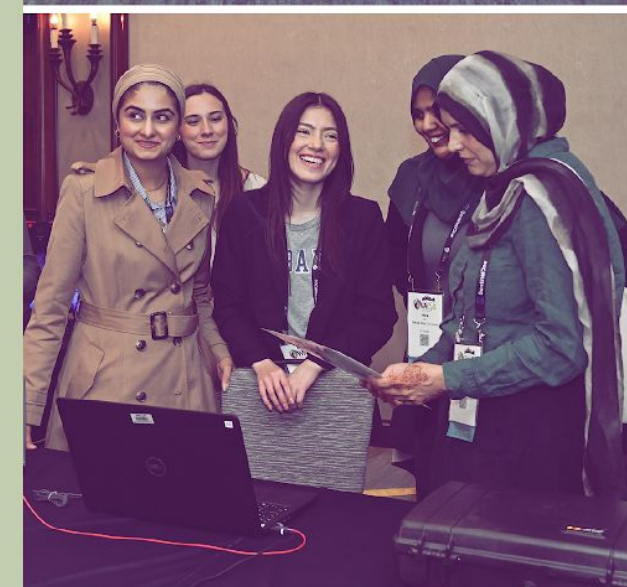
WiCyS 2026 *Conference*

#WiCyS2026

Call for Presenters
Call for Scholarships
Call for Volunteers

IN-PERSON
March 11-13

VIRTUAL
April 22-23



Call For Presenters (CFP) Timeline

Submissions Opened:
September 10, 2025

Submission Deadline:
October 15, 2025
5:00 PM Central Time (CT)

**Student Posters Deadline:*
December 15, 2025 at 5:00 PM CT

Notification of Status:
December 3, 2025

**Student Posters Notification: January 12, 2026*

CALL FOR *Presenters*

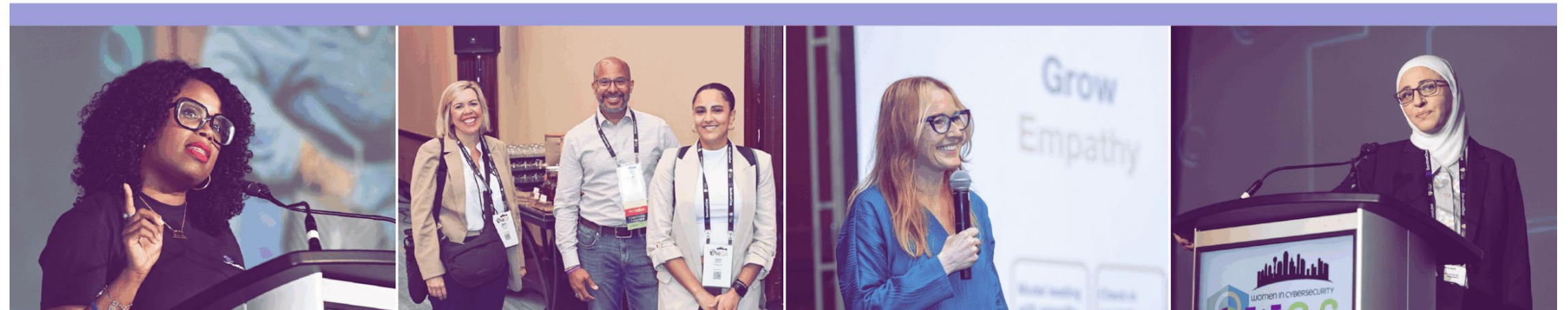
Workshop
Presentation
Lightning Talk

Panel
Birds of a Feather
Student Poster

Deadline to Submit is October 15

IN-PERSON
March 11-13
VIRTUAL
April 22-23

#WiCyS2026



Call For Presenters (CFP) Tracks (Updated for 2026)

- **Technical Skill Building** - technical skill development in all areas of cybersecurity and/or privacy
Example: A workshop on secure coding practices for AI-integrated applications.
- **Research and Innovation with Emerging Techniques** - scientific research addressing real-world cybersecurity challenges
Example: A study evaluating the effectiveness of biometric authentication against AI attacks.
- **Tools, Trends, Perspectives, and Sector-specific applications** - cybersecurity tools with specialized use cases across domains
Example: A threat modeling application tailored for healthcare providers.
- **Education, Workforce Development and Community** - all levels of cybersecurity education and training programs, strategies and initiatives for current and upcoming job demand
Example: A hands-on K-12 cybersecurity curriculum designed for after-school programs.
- **Career Development, Advancement & Management** - internships, apprenticeships and job search techniques, leadership, career development/growth, and personal wellness
Example: A hands-on session exploring job searching strategies using AI tools.

Call For Presenters (CFP) Mentor Program

If you are new to submitting a Call for Presenter or just need an extra dose of encouragement, please lean in on the **WiCyS CFP mentors**.

To request a mentoring session, email program@wicys.org.

The deadline to request a mentor is **October 1, 2025**.



Panels



PANELS

Panels provide opportunities to spotlight discussion on a current, relevant topic in cybersecurity and/or privacy. Panel submitters are responsible for selecting appropriate panelists to participate. In addition to the moderator, there can be two or three panelists and each panel is 45 minutes long with a minimum of two and a maximum of three panelists and one moderator listed. Submit all confirmed names and their affiliation info along with the abstract.

Being the Force Multiplier: Conversations on Careers in Cybersecurity Education

Moderator: *Paige Zaleppa*

Speaker(s): *Litany Lineberry, Elizabeth Rasnick and Barbara Clark*

Room: Grapevine C

Track(s): ● ●

Career Level: All

CPE Credits: 1

As the demand for skilled cybersecurity professionals continues to grow, it is essential to cultivate a strong pipeline of educators equipped to address the challenges of this evolving field. This discussion will focus on strategies to attract students to a career in teaching, retain mid-career educators, and demonstrate how educational leaders can provide support. Presenters will address the challenges educators face in the rapidly changing cybersecurity landscape and explore ways they successfully navigated these obstacles. Central to their mission is the commitment to inspiring and supporting aspiring faculty, ensuring no one is teaching in silos and that there is a strong connection to workforce needs. By engaging with the cybersecurity education ecosystem, the presenters aim to generate an affinity group of education leaders dedicated to nurturing new and early-career faculty. Attendees will gain insights into creating and participating in supportive communities for new, early-career and aspiring faculty, and the importance of mentorship in fostering professional growth. Participants will be encouraged to actively engage during the session. Together, this session aims to build a strong foundation for developing faculty that equip students with the necessary knowledge and skills to navigate the complexities of the cybersecurity landscape.

Mastering Incident Response: Practical Insights and Strategies

Moderator: *Shannon McCormick*

Speaker(s): *Julia Down and Shireen Jaffer*

Room: Grapevine D

Track(s): ●

Career Level: Early/Mid

CPE Credits: 1

When incident response is handled poorly, it often makes headlines. But what about the successes, where incident response shines behind the scenes? In the IR community, they frequently dissect high-profile failures and debate potential improvements. While learning from mistakes is invaluable, sharing any successes can also strengthen the entire field. This panel brings together experienced professionals who will discuss real-world examples of IR done right, highlighting the strategies, frameworks and techniques that led to effective resolutions. The panelists, representing a range of backgrounds, will share firsthand accounts of their incident response journeys; discussing pivotal moments, challenges faced and best practices refined through experience. For those new to incident response, this discussion will provide an introduction to IR fundamentals while seasoned professionals will gain fresh perspectives on elevating existing approaches. Join this session dedicated to mastering IR, where practical insights and strategies come together to build a stronger, more resilient community.

Examples

Panel Notes



PANELS

Panels provide opportunities to spotlight discussion on a current, relevant topic in cybersecurity and/or privacy. Panel submitters are responsible for selecting appropriate panelists to participate. In addition to the moderator, there can be two or three panelists and each panel is 45 minutes long with a minimum of two and a maximum of three panelists and one moderator listed. Submit all confirmed names and their affiliation info along with the abstract.

- 5 Sessions available
- 45 minutes duration
- Maximum 3 panelists and 1 moderator; minimum 2 panelists and 1 moderator
- Panelists with different backgrounds and viewpoints on the topic
- Clear takeaways from the panel discussion

- Moderator receives ***complimentary registration*** and does **not** receive Gaylord National Harbor Credit.
- Up to **three** panelists receive ***reduced rate conference registration*** (\$300) and do **not** receive Gaylord National Harbor Credit.
- Only presenters in attendance will be listed for the session.

Birds of a Feather (BoaF)

Cybersecurity and Work-Life Balance: Managing Stress and Avoiding Burnout

Speaker(s): *Katrina Xander*

Room: Grapevine D

Track(s): ●

Career Level: All

This session offers an open discussion on managing work-life challenges in a demanding field. Participants are invited to share experiences, insights and personal strategies for achieving balance between their personal and professional lives. Facilitators will guide conversations on best practices for setting boundaries, building resilience and creating a wellness-focused workplace culture. Attendees will discuss ways to manage cybersecurity's unique stresses, reduce burnout, and foster supportive environments where work-life balance is not only possible but encouraged. This session provides a space for professionals to connect, share, and learn how to make cybersecurity a sustainable and rewarding career path. Participants will leave with practical steps to improve their own work-life balance and to support their teams in managing stress, contributing to a healthier, more resilient workforce in cybersecurity.



BIRDS OF A FEATHER (BOAF)

Birds of a Feather (BoaF) are informal discussion sessions engaging the audience and moderated by the facilitator(s) on just about any topic related to cybersecurity and/or privacy. The facilitator leads the discussion with primary participation from the audience. These sessions can be a great way to share ideas and be introduced to current issues or trends in this area. BoaF sessions are 45 minutes long with a maximum of two listed facilitators.

Securing Emerging Technologies: Navigating the Risks of Tomorrow

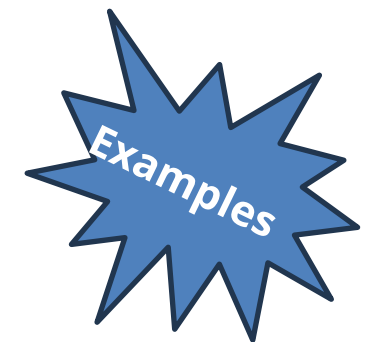
Speaker(s): *Neetu Jain and Fatima Ahmed*

Room: Grapevine B

Track(s): ●

Career Level: All

As the pace of technological advancement accelerates, new innovations bring both exciting opportunities and significant cybersecurity challenges. This session will focus on the security risks that arise with the adoption of emerging technologies. Facilitators will guide a discussion on how to proactively address these risks and develop strategies for integrating security into these technologies. Attendees will have the chance to share their experiences, discuss real-world scenarios and collaborate on potential solutions.



Birds of a Feather (BoaF) Notes



BIRDS OF A FEATHER (BOAF)

Birds of a Feather (BoaF) are informal discussion sessions engaging the audience and moderated by the facilitator(s) on just about any topic related to cybersecurity and/or privacy. The facilitator leads the discussion with primary participation from the audience. These sessions can be a great way to share ideas and be introduced to current issues or trends in this area. BoaF sessions are 45 minutes long with a maximum of two listed facilitators.

- **5 Sessions available**
- **45 minutes duration**
- **Maximum 2 presenters**
- Must be interactive
- Must encourage audience interaction throughout the whole session

- The **first** listed presenter receives ***complimentary registration*** and does **not** receive Gaylord National Harbor Credit.
- Other listed presenter do **not** receive complimentary registration or Gaylord National Harbor Credit.
- Only presenters in attendance will be listed for the session.

Posters



STUDENT POSTERS

Posters provide opportunities for students to present their work to the audience at WiCyS in poster format. The Poster judging process will select winners in both the undergraduate and graduate categories. The Winners of the poster competition in both undergraduate and graduate categories receive travel support for future security conference(s) of their choice. Runners-up receive prizes as well.

Exploring Large Language Models for Secure Computer Task Automation

Malak Mahdy, Texas A&M University, Corpus Christi

Large language models (LLM) are increasingly deployed in LLM-Powered Applications (LPA) to automate complex tasks across various domains. This research evaluates the potential of different LLM as autonomous agents in simulated forensic work environments by focusing on their ability to successfully complete tasks while maintaining security integrity. By analyzing the performance of LPA in sensitive scenarios, this study identifies strengths, limitations and vulnerabilities, providing insights to enhance the reliability and security of LLM-based systems for critical applications.

Examples

RiFT: Simulating Cyberattacks on Critical Infrastructure to Identify Potential Risks

Aashi Agarwal, Purdue University

The Cybersecurity and Infrastructure Security Agency identifies 16 critical infrastructure sectors that are vital to national security, economy, and public health and safety. Our goal was to estimate the potential risks associated with cyberattacks on three of these critical infrastructure sectors: healthcare, energy, and water and wastewater. We developed models of these systems using an object-oriented programming approach (Java) in the AnyLogic software package. Due to the dependencies between sectors, we also analyzed the cascading impacts of attacks in one sector on other sectors by building a combined unified model. Using our models for simulation, we can easily configure different parameters for systems and adversaries and measure the associated risks. This improved understanding of the potential risks associated with cyberattacks on critical infrastructure helps us develop effective cyber-defenses and mitigations.

Student Poster Competition



STUDENT POSTERS

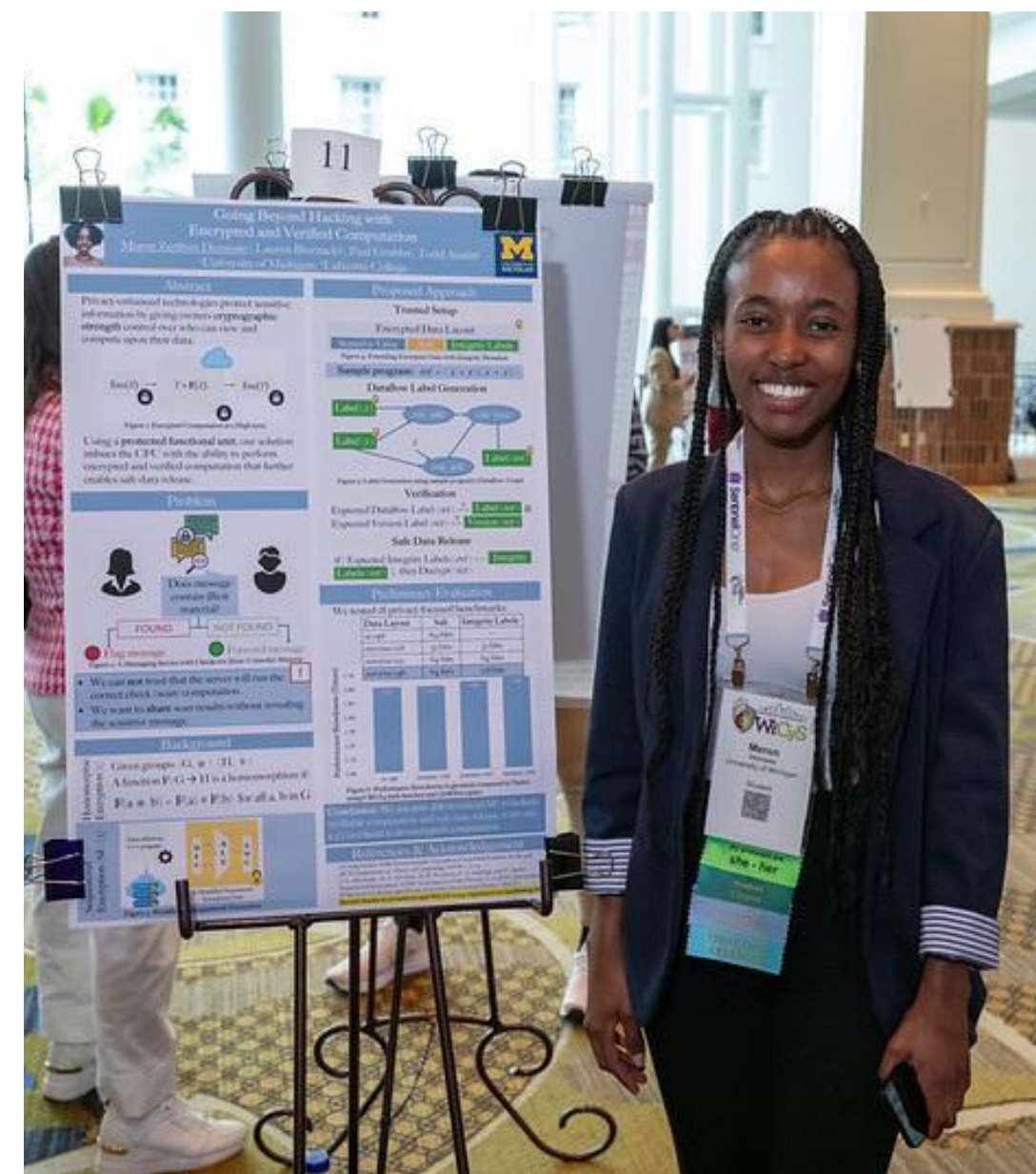
Posters provide opportunities for students to present their work to the audience at WiCyS in poster format. The Poster judging process will select winners in both the undergraduate and graduate categories. The Winners of the poster competition in both undergraduate and graduate categories receive travel support for future security conference(s) of their choice. Runners-up receive prizes as well.

- **Two categories:** Undergraduate and Graduate
- First listed researcher and presenter must be a female student
- Can be about work-in-progress

- The **first** listed student of accepted poster will receive an automatic scholarship with benefits.
- Additional students listed on a poster must apply for a scholarship to attend and there is no automatic scholarship.
- Submissions must be presented in person and the first listed presenter must be the lead presenter.

Accepted poster presenters must become a student member to receive WiCyS conference scholarships (if they are not already a student member).

Some Past Poster Presenters



Poster Session Notes



STUDENT POSTERS

Posters provide opportunities for students to present their work to the audience at WiCyS in poster format. The Poster judging process will select winners in both the undergraduate and graduate categories. The Winners of the poster competition in both undergraduate and graduate categories receive travel support for future security conference(s) of their choice. Runners-up receive prizes as well.

- **Highlight major points of research/work**
 - Why is the work important?
 - What is the work about?
 - What approach is used?
 - What is the outcome/next steps?

Workshops



WORKSHOPS

Workshops are hands-on sessions (technical/professional development) on any topic related to cybersecurity and/or privacy. The audience should be engaged and participate in activities throughout the session. Workshops are 1 hour and 45 minutes in length with a maximum of four listed presenters. Workshops should be suitable for a large audience (>150 attendees).

Hands On SOC Workshop: Mastering Cyber Threat Detection and Response

Speaker(s): Paula De Albuquerque, Shaabena Abdul Ghani and Mandeep Malhi

Room: Grapevine B

Hands On Workshop

Career Level: Early/Mid

Track(s): ●

Laptop Required

CPE Credits: 2

Step into the world of Security Operations Center (SOC) roles in this hands-on workshop designed to equip participants with practical, real-world cybersecurity skills. This session offers an immersive experience where attendees will navigate the daily responsibilities of SOC analysts through the Challenge Lab - an engaging component of the presenting company's official SOC training. Participants will rotate through red, blue and purple team roles, starting with red, to emulate adversary tactics, techniques and procedures (TTPs) in a simulated attack scenario. As they shift to blue, attendees will validate detection capabilities on specific security products and carry out incident-handling activities following NIST SP 800-61 guidelines. Leveraging one of the security products' orchestration capabilities, participants will analyze incidents and implement response measures, gaining critical insights into detection and response processes. In the final purple team role, participants will compile a comprehensive report to summarize findings and recommend enhancements to the organization's security posture, bridging the gap between attack and defense strategies. This workshop is ideal for students, cybersecurity newcomers and professionals looking to deepen their SOC expertise through active, hands-on learning. By engaging in these real-world scenarios, attendees will develop confidence and operational skills in threat detection, incident response and security management directly aligned with industry standards. Gain experience in cybersecurity's front lines and connect with a community dedicated to advancing practical knowledge and closing the cybersecurity skills gap.

Blueprint for AI-Powered Resilience: Embedding Secure by Design for Next-Gen Cyber Defense

Speaker(s): Yasmin Abdi

Room: Grapevine C

Hands On Workshop

Career Level: All

Track(s): ●

Laptop Required

CPE Credits: 2

In a world of rapidly evolving cyber threats, traditional defenses are no longer enough to safeguard critical systems and data. This workshop offers an innovative approach to fortifying cybersecurity architectures by embedding AI-driven, Secure by Design principles from the ground up. Participants will gain insight into how AI can proactively strengthen defenses, automate threat detection, and adapt systems to withstand increasingly sophisticated attacks. Through interactive, hands-on exercises, attendees will collaborate in industry-focused groups - healthcare, finance, retail and government - to design custom, resilient architectures tailored to real-world challenges unique to each sector. Each team will work with evolving threat scenarios, requiring real-time adjustments and strategic design thinking to build adaptive, secure solutions. This immersive experience not only highlights the practical integration of AI but also showcases how Secure by Design principles enhance resilience over time. Led by experts in security engineering, consulting, governance, risk and compliance, this session ensures that participants leave with actionable skills and a clear roadmap for implementing AI-enhanced, industry-specific cyber defenses. By providing a unique, scenario-based approach, this workshop empowers professionals to anticipate threats, address vulnerabilities and construct future-proof security architectures.

Workshop Notes

- **14 Sessions available**
- **1 hour 45 minutes duration**
- **Maximum 4 presenters**
- **Suitable for large audience >150**
- Submission should state if attendees need to bring laptops
 - Any additional software needed must be noted in the submission



WORKSHOPS

Workshops are hands-on sessions (technical/professional development) on any topic related to cybersecurity and/or privacy. The audience should be engaged and participate in activities throughout the session. Workshops are 1 hour and 45 minutes in length with a maximum of four listed presenters. Workshops should be suitable for a large audience (>150 attendees).

- The **first** listed presenter receives ***complimentary registration and Gaylord National Harbor Credit.***
- The **second** listed presenter receives ***complimentary registration*** and does **not** receive Gaylord National Harbor Credit.
- Other listed presenters receive ***early registration*** and do **not** receive complimentary registration or Gaylord National Harbor Credit.
- Only presenters in attendance will be listed for the session.

Lightning Talks

Using Role-Play to Increase Engagement in Cybersecurity Classrooms

Speaker(s): Victoria Berkowitz

Sometimes learning technical skills can be daunting! Pair this with imposter syndrome and you may have a learning session turn sour. Ever sit through a technical session and say to yourself, "Why am I learning this?" The answer should be more than, "just because it is important." Teaching technical skills is critical, but teaching why and how they are used is even more important. Making learning engaging and tangible is key to recruiting, retaining and advancing women in cybersecurity. Tune in to hear how simple gamification tools like role-play/simulation can help make more engaging and meaningful learning!

Breaking News: How Cybersecurity Media Shapes the Industry

Speaker(s): Nancy Chenyizhi Liu

Cybersecurity news media plays a crucial yet often overlooked role in the industry, acting as the bridge between real-time developments, expert insights and the broader community. This session will explore how trusted news outlets shape industry discussions, provide vital updates on emerging threats, and foster collaboration among cybersecurity professionals. Attendees will learn how media breaks down complex security topics for non-technical audiences, ensuring that the general public, businesses and even government entities stay informed about critical issues. The session will highlight how accurate, timely reporting is essential for effective threat response and the challenges posed by misinformation and



LIGHTNING TALKS

Lightning talks highlight fresh ideas, unique perspectives, valuable experiences and emerging trends in cybersecurity and/or privacy. Lightning Talks are *five-minute talks* (with or without formal presentations) with a maximum of one listed presenter.

sensationalism in cybersecurity coverage. By the end of this talk, participants will have a better understanding of how to engage with cybersecurity media to stay informed, contribute to industry discussions, and leverage news outlets as tools for both education and advocacy. The session also will examine the importance of timely and accurate reporting in enabling effective threat responses, as well as the challenges posed by misinformation and sensationalism in cybersecurity news. By the end of the talk, participants will gain a deeper understanding of how to engage with cybersecurity media to stay informed, contribute to industry discussions, and leverage the media as a tool for education and advocacy.

AI-Powered Cyber Range

Speaker(s): Varshitha Manjunath

In the rapidly evolving landscape of cybersecurity, traditional static training scenarios often fall short in preparing professionals for real-world threats. This session introduces an innovative approach: leveraging Large Language Models (LLMs) to create AI-powered cyber ranges with dynamic, adaptive training scenarios. Attendees will explore how LLMs can generate diverse, realistic cyber attack simulations that evolve in response to learner actions, mirroring the unpredictability of actual security incidents. This approach promises to enhance engagement, improve skill retention, and accelerate the development of critical thinking in cybersecurity professionals.

Examples

Lightning Talks Notes



LIGHTNING TALKS

Lightning talks highlight fresh ideas, unique perspectives, valuable experiences and emerging trends in cybersecurity and/or privacy. Lightning Talks are **five-minute talks** (with or without formal presentations) with a maximum of one listed presenter.

- 16 Sessions available
- 2 sessions of 8
- Maximum of 5 minute presentation
- Maximum 1 presenter
- Great for new speakers
- Can be about work-in-progress

- The **first** listed presenter receives ***complimentary registration*** and does **not** receive Gaylord National Harbor Credit.

Presentations



PRESENTATIONS

Technical presentations highlight innovations, research & development projects, technical skills development, internships/co-ops experiences, service-learning and outreach projects, or other interesting experiences related to cybersecurity and/or privacy. Technical presentations are 45 minutes long, including time for Q&A, with a maximum of two listed presenters.

The Impact of Quantum-Safe Cryptography on Website Response

Speaker(s): Ananya Tadepalli

Room: Grapevine A

Track(s): ●

Career Level: All

CPE Credits: 1

Modern web traffic relies on 2048-bit RSA encryption to secure our data in transit. Rapid advances in quantum computing pose a grave challenge by allowing hackers to break this encryption in hours. In August 2024, the National Institute of Standards and Technology published Quantum-Safe Cryptography (QSC) standards, including CRYSTALS-Kyber for general encryption and CRYSTALS-Dilithium, FALCON and SPHINCS+ for digital signatures. Despite this proactive approach, the slow adoption of encryption protocols remains a concern, leaving a significant portion of data vulnerable to interception. In this context, this study aims to evaluate the impact of NIST's quantum-resistant cryptographic algorithms on website response times, particularly focusing on SSL handshake time and total download time under varying network conditions. By assessing the performance of these algorithms, this research seeks to provide empirical evidence and a reusable framework for validating the efficacy of QSC in real-world scenarios. It was found that the QSC algorithms outperformed the classical algorithm under normal and congested network conditions. Also discovered was an improvement in the total download time for larger file sizes and a better performance by QSC under higher latency and packet loss conditions. This study recommends that websites switch to QSC when the standards are ratified. These insights are crucial for accelerating the adoption of QSC and ensuring the security of data in the face of quantum computing threats.

Unlocking Funding: Navigating Scholarships and Support in Cybersecurity

Speaker(s): Angela Clark and Rebecca Clark

Room: Grapevine B

Track(s): ●●

Career Level: All

CPE Credits: 1

Unlock cybersecurity potential by joining this dynamic presentation focused on funding opportunities for aspiring students! This session will cover a comprehensive range of sources available for scholarships, grants and sponsorships specifically tailored to cybersecurity studies. Attendees will learn effective application strategies to create compelling submissions that capture the attention of funding committees. Additionally, the session will explore proven networking techniques to connect with industry professionals and organizations that can provide guidance and support throughout one's journey. Whether just starting out or looking to advance studies, this presentation will equip attendees with the essential tools and insights to secure the financial resources needed to succeed in the cybersecurity field. Session leaders include a university faculty member who has mentored numerous students and manages a cybersecurity scholarship program and an NSF graduate research fellow who has been awarded various scholarships to support her cybersecurity studies. Don't miss this opportunity to invest in the future!

Examples

Presentation Notes



PRESENTATIONS

Technical presentations highlight innovations, research & development projects, technical skills development, internships/co-ops experiences, service-learning and outreach projects, or other interesting experiences related to cybersecurity and/or privacy. Technical presentations are 45 minutes long, including time for Q&A, with a maximum of two listed presenters.

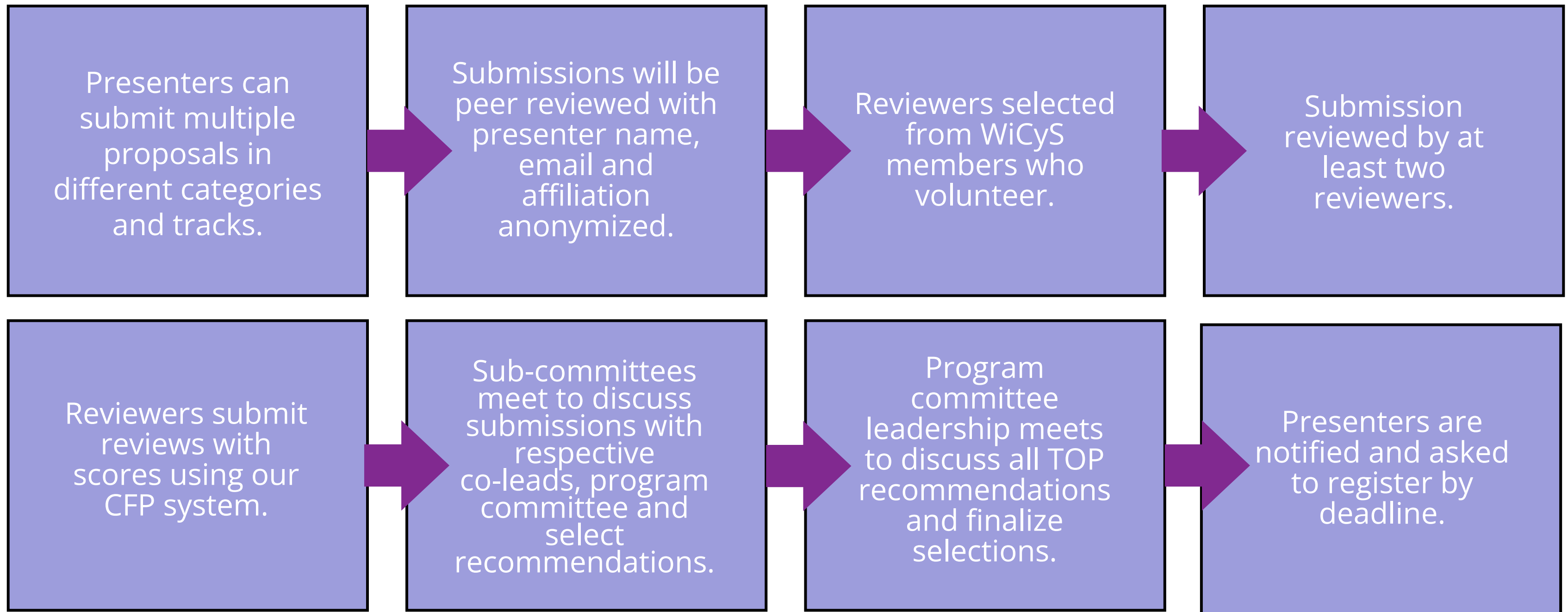
- **30 Sessions available**
- **45 minutes duration**
- **Maximum 2 presenters**
- Audience interaction is limited to 10 min Q&A

- The **first** listed presenter will receive ***complimentary registration*** and **Gaylord National Harbor Credit**.
- The **second** listed presenter receives ***complimentary registration*** and does **not** receive Gaylord National Harbor Credit.
- Only presenters in attendance will be listed for the session
- If accepted for Virtual Conference: first and second listed presenters receive complimentary virtual conference registration.

Top 10 Reasons to Submit to WiCyS CFP

1. Be seen and heard at the largest world stage that spotlights women in cybersecurity.
2. Showcase your talent/work at the conference that brings industry, government, and academia together.
3. Share with your community your knowledge/experiences.
4. Sharpen your skill as presenter.
5. Great venue for 1st timers and old timers!
6. Feel at home with your own community.
7. Inspire others like you.
8. Help to recruit, retain and advance more women in cybersecurity.
9. Help your community advance.
10. Because YOU need to be heard and seen!

Submission Selection Process



Selection Goals

Balance program portfolio
across tracks and categories

No repeat of the same
content from recent WiCyS
conferences

Provide opportunities to
presenters across different
backgrounds and
organizations

Quality is the topmost
priority!!!

Rubric

1. Content is **relevant to cybersecurity/privacy** or **career-development** in the area of cybersecurity/privacy.
2. Content is **relevant to one of the tracks** (Technical Skill Building; Research and Innovation with Emerging Techniques; Tools,Trends, Perspectives, and Sector-specific applications; Education, Workforce Development, and Community; Career Development, Advancement, and Management).
3. Content is **technical** (for technical topics) or **thought provoking** (for non-technical topics).
4. Content is **timely**.
5. Content is **creative and innovative**.
6. Content clearly **addresses a problem or solution or both**.
7. Content has **clear take-aways or research outcomes for the audience**.
8. Session is **engaging for the attendees**.
9. Abstract **description** is well articulated and provides a clear overview of the content.
10. **Outline** provides a good view of session content, activities, and outcomes.

General Tips for Submissions

Relevant and Specific

- To topics in cybersecurity and privacy
- Matched to one or more tracks and tailored to the category
- To career development/advancement of cyber professionals
- Not everything needs to apply to females in cybersecurity
- No “vendor” pitch in proposal submission
 - Technology Showcase with tools demonstrations are offered by sponsors

To the point (Not lengthy)

- Describe specifically what the presentation will address
- Be within 250 words for overview/abstract (to be published in the conference program)
- Provide additional information about presentation outline (not published)
- Absolutely NO information about submitters(s)/presenter(s) identity (name or affiliation/association of institution/company) in the body of proposal; may talk about experience/qualifications

Written in Third-person

- Example:
 - Don't say: I will talk about it
 - Do say: This talk will present/discuss

CFP Submission Site Review

CALL FOR *Presenters*

Workshop
Presentation
Lightning Talk

Panel
Birds of a Feather
Student Poster

IN-PERSON
March 11-13

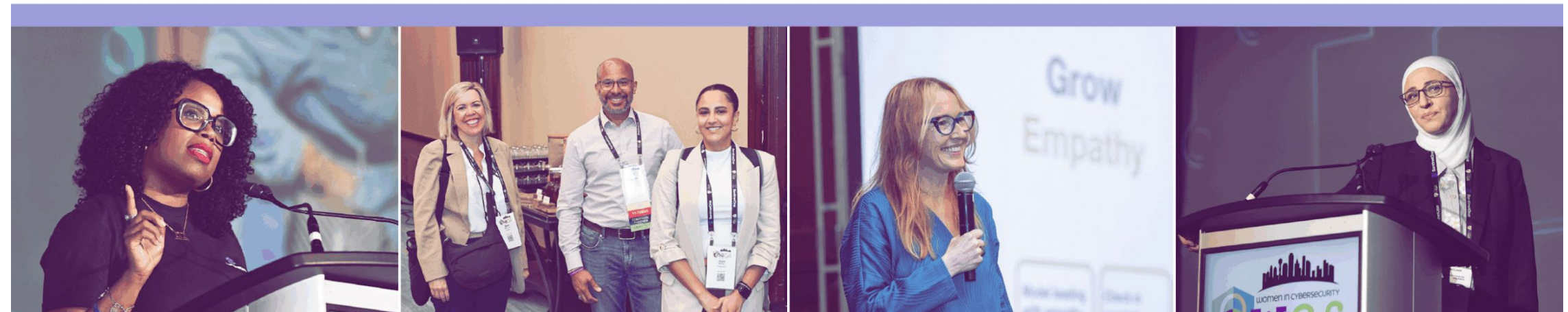
VIRTUAL
April 22-23

#WiCyS2026



Timely
Innovative
Unique perspective
Engaging
Clear takeaways
Addresses a problem/challenge

Deadline to Submit is October 15



CFP Webinar Panel



Betta Lyon Delsordo



Heather Holliday



Linxi Zhang



Suzanne Dove

Reminders

Submission through WiCyS CFP portal
(Deadline October 15, 2025 at 5 PM Central Time CT)

WiCyS 2026 Call For Presenters:

<https://www.wicys.org/events/wicys-2026/call-for-presenters>



- Anyone can submit
- Review feedback provided
- Presenters must register by deadline
- Mentoring request is available until October 1, 2025
- Accepted presenters must register by deadline



**“Alone we are smart.
Together we are brilliant.”
— Steven Anderson**

For more information, contact:
program@wicys.org

