WiCyS 2025 Conference CFP (Call for Presenters) Resource Deck

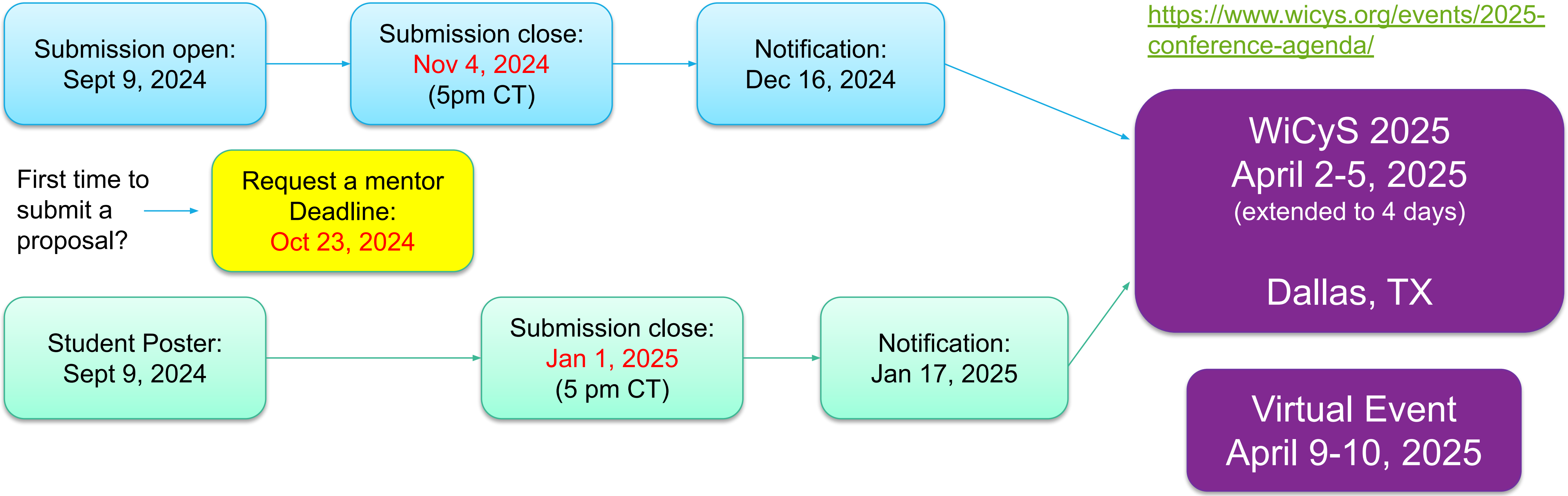
Jennifer Cheung
https://www.linkedin.com/in/jennifercheung/

Sept 18, 2024

women in cybersecurity
WiCyS
SAN DIEGO
AFFILIATE

WiCyS 2025 Conference Submission Timeline

WiCyS 2025 agenda: https://www.wicys.org/events/2025-conference-agenda/



Submission open: Sept 9, 2024

Submission close: Nov 4, 2024 (5pm CT)

Notification: Dec 16, 2024

First time to submit a proposal?

Request a mentor Deadline: Oct 23, 2024

Student Poster: Sept 9, 2024

Submission close: Jan 1, 2025 (5 pm CT)

Notification: Jan 17, 2025

WiCyS 2025
April 2-5, 2025
(extended to 4 days)

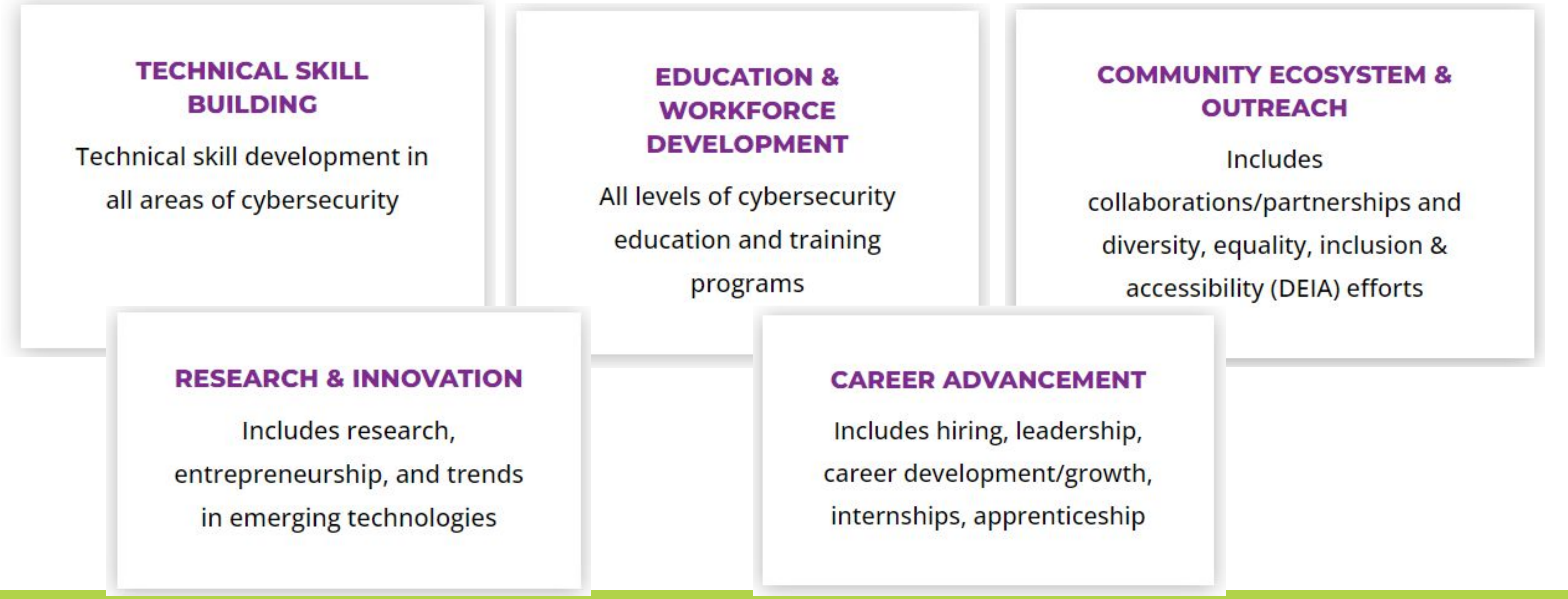
Dallas, TX

Virtual Event
April 9-10, 2025

Send mentor request or any questions to **program@wicys.org**

https://www.wicys.org/events/wicys-2025/call-for-presenter/

2025 - Five Tracks



TECHNICAL SKILL BUILDING

Technical skill development in all areas of cybersecurity

EDUCATION & WORKFORCE DEVELOPMENT

All levels of cybersecurity education and training programs

COMMUNITY ECOSYSTEM & OUTREACH

Includes collaborations/partnerships and diversity, equality, inclusion & accessibility (DEIA) efforts

RESEARCH & INNOVATION

Includes research, entrepreneurship, and trends in emerging technologies

CAREER ADVANCEMENT

Includes hiring, leadership, career development/growth, internships, apprenticeship

5 Proposal Categories + Student Poster

Technical Presentation
(45 mins)

Workshop
(2 hours)

Birds of a Feather (BOAF)
(45 mins)

Lightning Talk
(5 mins)

Panels
(45 mins)

Student Poster
(ongoing-one session)

https://www.wicys.org/events/wicys-2025/call-for-presenter/

Proposals Acceptance Rates

Type of proposal	Acceptance Rate 2022 (371-total)	Acceptance Rate 2023 (652-total)	WiCyS 2024 Available Slots (800+ total)	WiCyS 2025 Available Slots
Tech Presentation	11%	5.6%	16	34
Panel	15%	7.4%	5	5
Bird of A Feather (BoaF)	13%	11.9%	5	5
Lightning Talk	21.6%	23.9%	16	16
Workshop	34.6%	20.0%	19	26
Student Research Poster	38%	42.1%	28	TBD

Seeking first time submitters, always!

Proposal Categories & Benefits

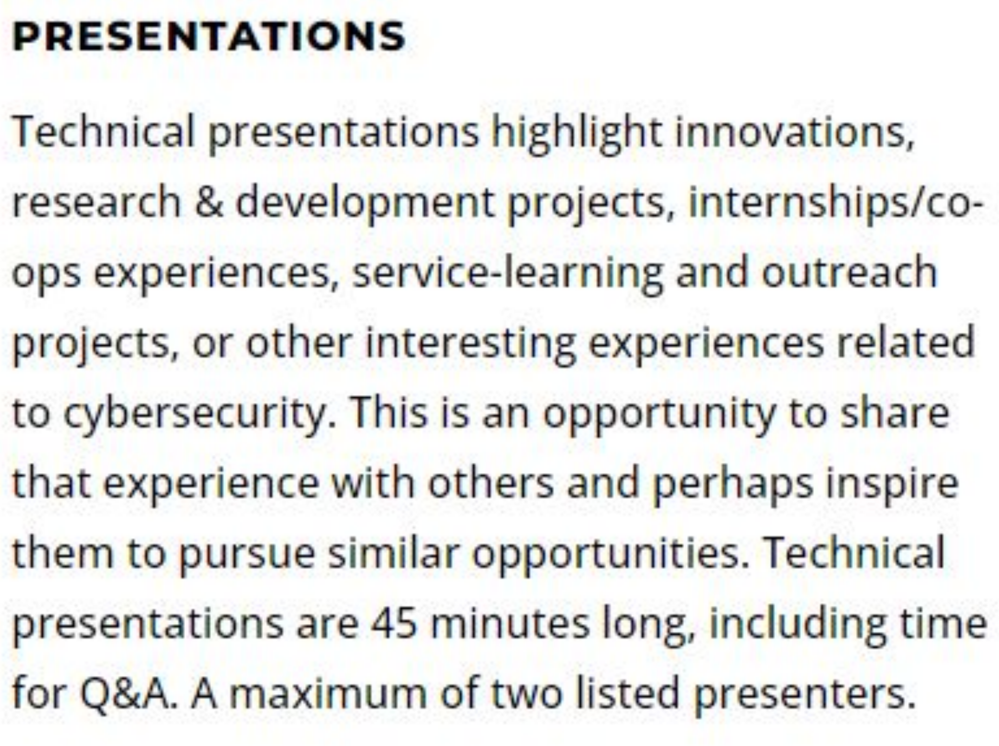
Proposal Category	Time limit	Presenter	Complimentary Registration	Complimentary Lodging (2 nights)	Early Registration
Tech Presentation	45 mins	2	1st & 2nd listed presenter	1st listed presenter	
Workshop	2 hours	Max 4	1st & 2nd listed presenter	1st listed presenter	
Bird of A Feather (BoaF)	45 mins	2	1st listed facilitator		2nd listed presenter
Lightning Talk	5 mins	1	Listed presenter		
Panel	45 mins	4 (1 mod)	Moderator	Up to 3 panelists-reduced rate registration ($300)	
Student Research Poster		Only WiCyS member	1st listed - Automatic Scholarship		

WiCyS 2025 Agenda - Tentative

April 2, 2025 (Wednesday)	April 3, 2025 (Thursday)	April 4, 2025 (Friday)	April 5, 2025 (Saturday)
	Main Sessions	Main Sessions	Main Sessions (Morning)
Pre Conference Workshops	Career Fair CTF After Dark	Career Fair Award Dinner	Post Conference Workshops

https://www.wicys.org/events/2025-conference-agenda/

Proposal Categories- Technical Presentation (45 mins)



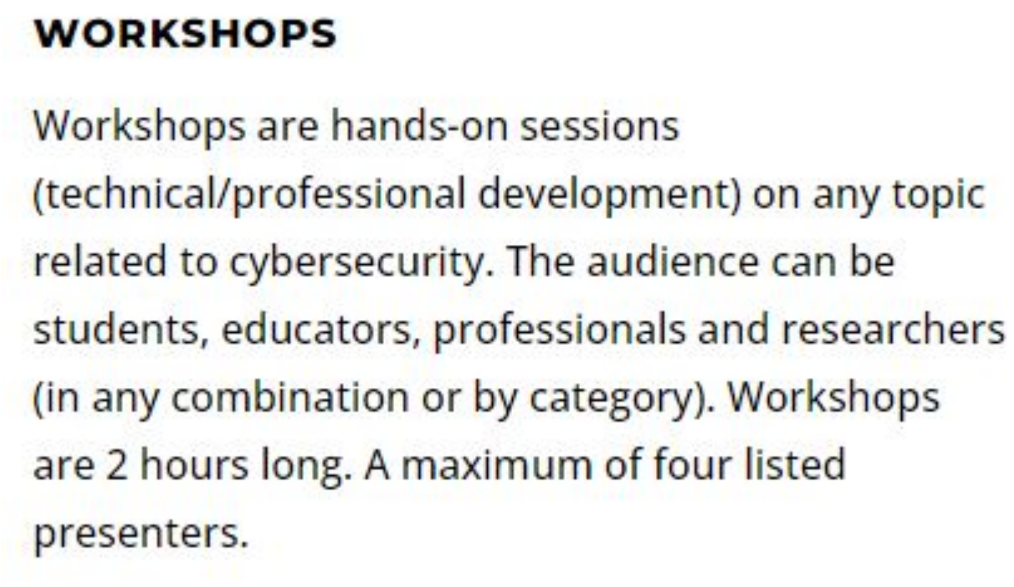
PRESENTATIONS

Technical presentations highlight innovations, research & development projects, internships/co-ops experiences, service-learning and outreach projects, or other interesting experiences related to cybersecurity. This is an opportunity to share that experience with others and perhaps inspire them to pursue similar opportunities. Technical presentations are 45 minutes long, including time for Q&A. A maximum of two listed presenters.

Example topics (2023):

- One Thousand Ways to Bypass MFA
- The Hacker Within, From IRC to Boardroom
- Introduction to AI Red Teaming
- PII: The Privacy Zombie
- Security Evaluation of Mental Health Care Applications and Web Services
- Stop the (OT) Apocalypse! Protecting the Nation’s Critical Infrastructure
- Building a Talent Pipeline with Staff Internships

Proposal Categories- Workshop (2 hours)



WORKSHOPS

Workshops are hands-on sessions (technical/professional development) on any topic related to cybersecurity. The audience can be students, educators, professionals and researchers (in any combination or by category). Workshops are 2 hours long. A maximum of four listed presenters.

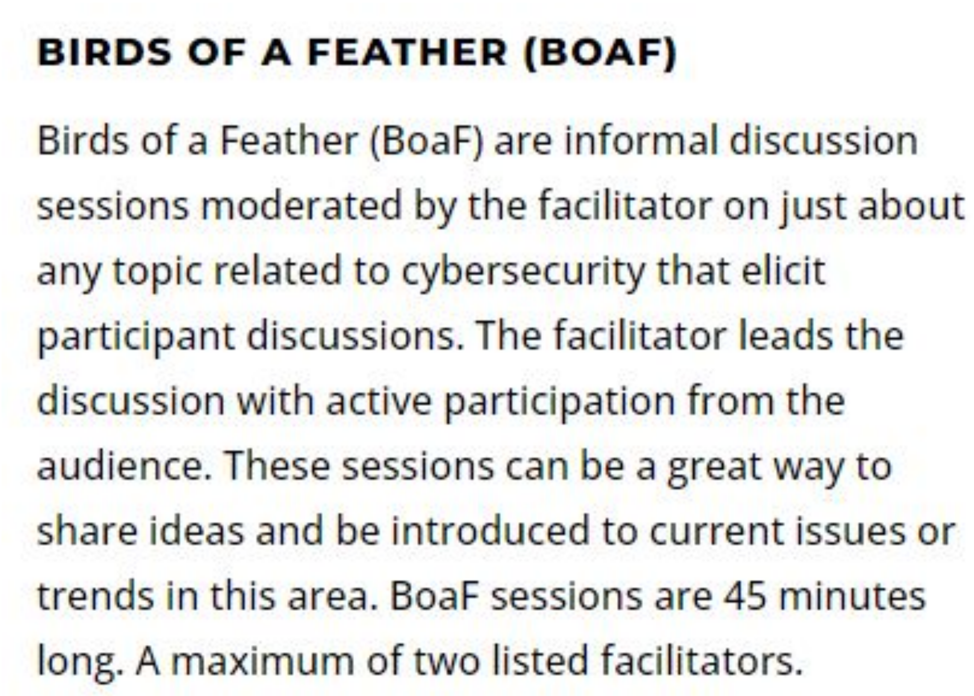
Example topics (2023):

Pre conf (Thurs afternoon)-
- AWS Security GameDay 2023
- Cybersecurity Career Exploration Via Virtual Reality

Main conf (Friday afternoon)
- Self Accountability and Challenging Our Own Bias
- Two Sides of a Coin: User Data Privacy, Security and Ethics of 5G Technology

Post conf (Sat afternoon)
- Attacking and Defending Public Cloud Environments
- CyberCareer Exploration (C2E) and Training for Transitioning Veterans and Military

Proposal Categories- Birds of a Feather (BOAF) (45 mins)



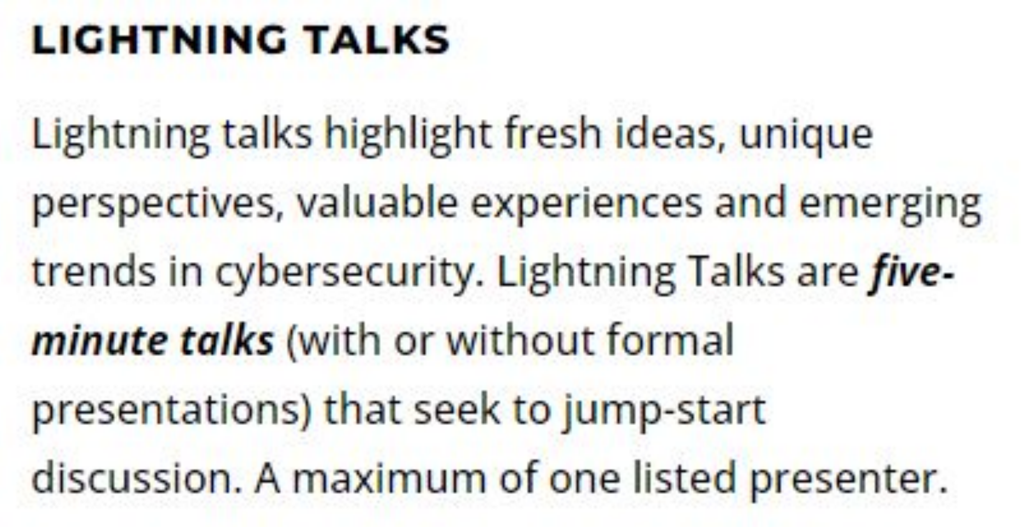
BIRDS OF A FEATHER (BOAF)

Birds of a Feather (BoaF) are informal discussion sessions moderated by the facilitator on just about any topic related to cybersecurity that elicit participant discussions. The facilitator leads the discussion with active 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. A maximum of two listed facilitators.

Example topics (2023):

- Security Research: Creating a Bridge Between Research Projects and Business Benefits
- Artificial Intelligence and Race: Security or Surveillance?
- Internships, Apprenticeships, Co-ops and Service Learning

Proposal Categories- Lightning Talk (5 mins)



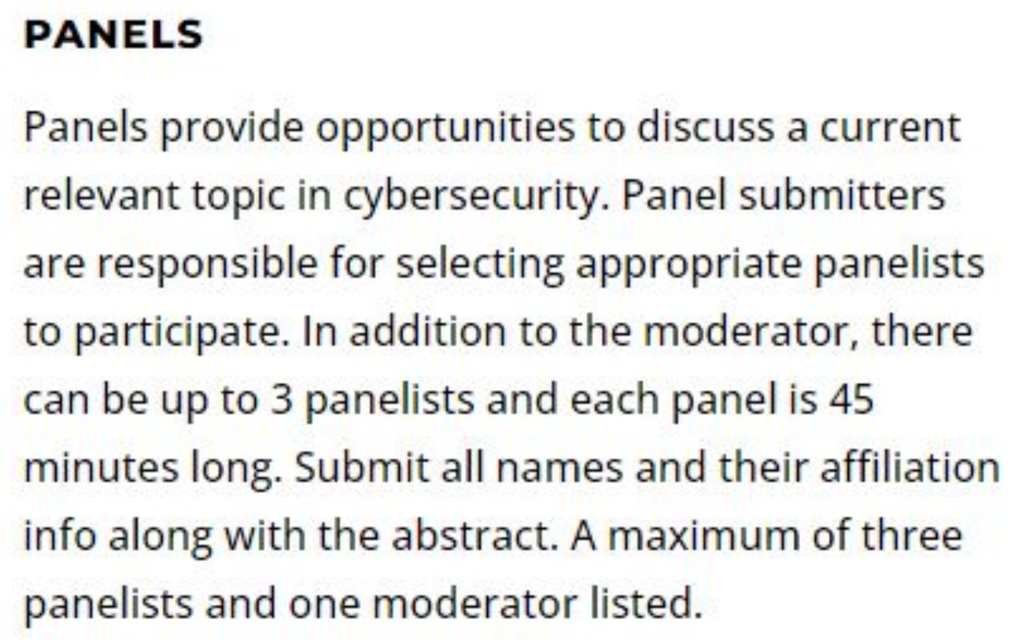
LIGHTNING TALKS

Lightning talks highlight fresh ideas, unique perspectives, valuable experiences and emerging trends in cybersecurity. Lightning Talks are ***five-minute talks*** (with or without formal presentations) that seek to jump-start discussion. A maximum of one listed presenter.

Example topics (2023):

- Making My Way Through Tech as a Neurodivergent, Queer, Woman of Color
- User and Entity Behavior Analytics: The Future of Advanced Threat Detection
- Great Student, Great Employee: How to Thrive During the Post-Grad Transition
- Cyber-Informed Engineering and the Future of OT Security
- Wait! They Said What? Hide Age and Years of Experience!
- Full Speed Ahead: Accelerating the DoD's Dominance with Cloud Native Security

Proposal Categories- Panels (45 mins)



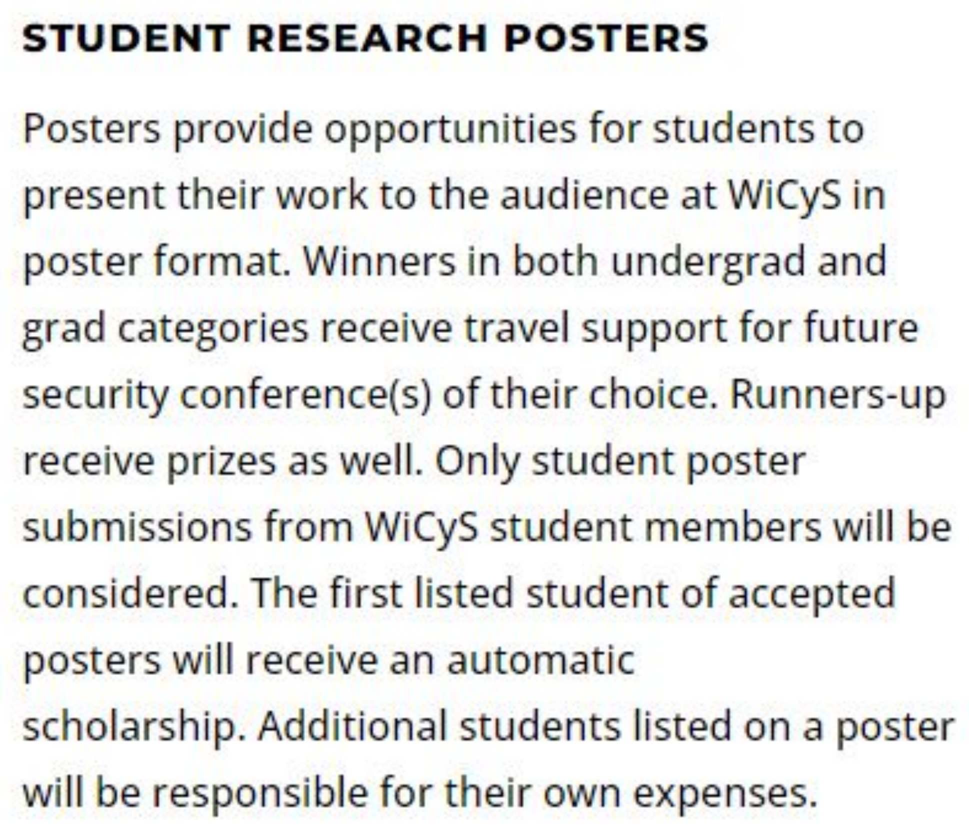
PANELS

Panels provide opportunities to discuss a current relevant topic in cybersecurity. Panel submitters are responsible for selecting appropriate panelists to participate. In addition to the moderator, there can be up to 3 panelists and each panel is 45 minutes long. Submit all names and their affiliation info along with the abstract. A maximum of three panelists and one moderator listed.

Example topics (2023):

- Flying High: The Women of Aerospace Cybersecurity
- CyberCrime Prevention and Investigation: A Case Study of Public, Private and University Partnership
- Politics, Partnerships and Incident Response

Proposal Categories- Student Posters (Undergrad / Grad)



STUDENT RESEARCH POSTERS

Posters provide opportunities for students to present their work to the audience at WiCyS in poster format. Winners in both undergrad and grad categories receive travel support for future security conference(s) of their choice. Runners-up receive prizes as well. Only student poster submissions from WiCyS student members will be considered. The first listed student of accepted posters will receive an automatic scholarship. Additional students listed on a poster will be responsible for their own expenses.

Example topics (27) (2023):

- Detection of Cyberbullying in GIF/Stickers Using AI
- A Framework for Identifying Malware Threat Distribution on the Dark Web
- Machine Learning Trust Management System for Blockchain Organ Donation Framework
- Automated CWE-Vulnerability Prediction Using Abstract Syntax Tree Embeddings
- Accelerating In-Vehicle Network Intrusion Detection System Using Binarized Neural Network

Exercise/Discussion Break (5-10 mins) -Think About What You Want to Submit

Which track you are submitting

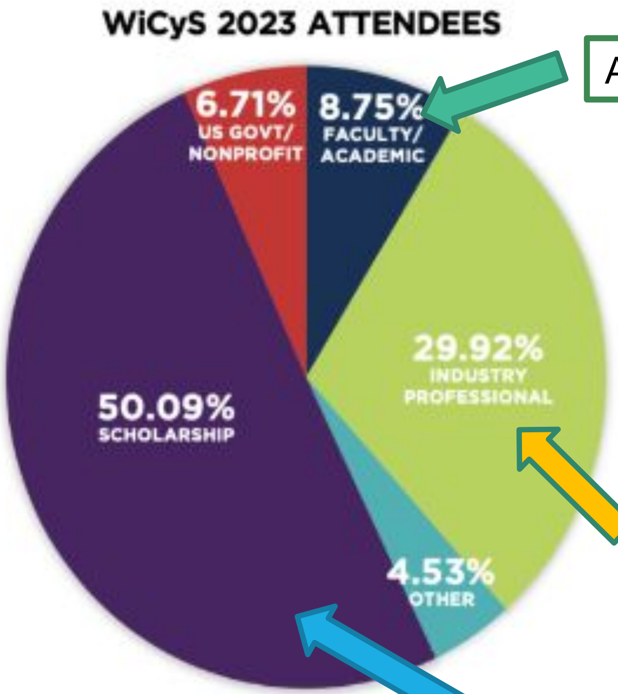
1. Technical Skill Building
2. Education & Workforce Development
3. Research & Innovation
4. Career Advancement & Management
5. Community Ecosystem & Outreach

Which type of proposals you are submitting

1. Tech Presentation (45 mins)
2. Workshop (2 hours)
3. BoaF-Bird of A Feather (45 mins)
4. Lightning Talk (5 mins)
5. Panel (45 mins)
6. Student Research Poster (WiCyS student members only)

Next step: write your abstract

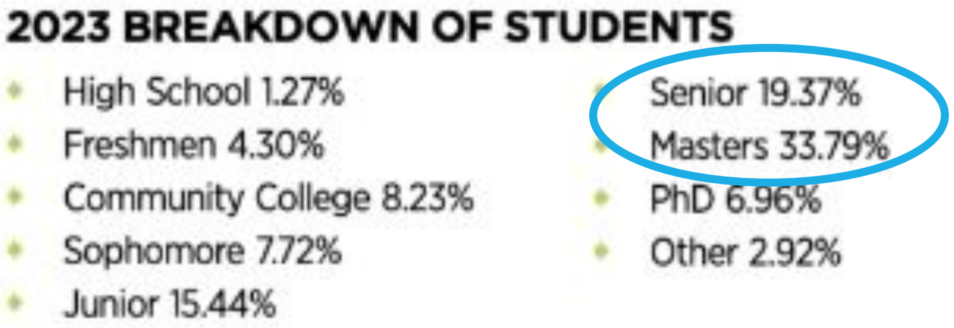
Write/Speak to Your Conference Audience



Academia

Industry / workforce development

~ 50% are students



2023 BREAKDOWN OF STUDENTS

- High School 1.27%
- Freshmen 4.30%
- Community College 8.23%
- Sophomore 7.72%
- Junior 15.44%
- Senior 19.37%
- Masters 33.79%
- PhD 6.96%
- Other 2.92%

WiCyS 2024 Conference Evaluation Report:
https://www.wicys.org/wp-content/uploads/2024/08/WiCyS-2024-Evaluation-Report-External_8.24.24.pdf

Proposal Content—Abstract / Outline

Abstract (Required, up to 250 words)

- Overview that describes the offering
- To be published in conference program

Outline (Required, up to 500 words, not published)

- Additional relevant info
- Articulates plan/outline of presentation

Author Info (Blind)

- DO NOT mention name or company/affiliation of author(s)
- OK to mention: presenter’s experience related to the topic

General Tips:

Relevant and Specific

- Topic □ cybersecurity
- Not everything needs to apply to female in cybersecurity
- No vendor pitch

To the point (be precise)

- Describe specifically what the presentation will address
- May provide additional info about presentation outline

Written in Third-person

- This talk will present / discuss
- Don’t say: I will talk about…

Selection Process & Rubric

- Author can submit multiple proposals in different categories and tracks
- Submissions will be peer reviewed **blindly** (without name, email and affiliation)
- Submission scored by at least two reviewers
- Sub-committee on each categories meets and discuss submissions with co-lead and select recommendations for Program Committee (PC) Leadership
- PC leadership meets to discuss all recommendations from sub-committees and finalize selections
- Authors will be notified on Dec 16, 2024 and ask to register.

Content is

- Compelling / timely
- Technical sound
- Relevant to the tracks

Title

- Provide good indication of content of session

Description

- Is well articulated and written
- Provides good view of session content, activities and outcomes.

CFP Guidance – 7 Tips

Understand the conference focus

- The five tracks

Look at sample successful CFPs

- ✓ 2022 conference program
- ✓ 2023 conference program
- ✓ 2024 conference program

Make it interesting

- Share your enthusiasm for the topic
- Convey your authenticity
- ✓ Story telling

Include key items

- Include primary research that aligns with the conference audience
- Share what the problem is, the solution and what you are going to present

Provide actionable recommendations

- What are the attendees going to learn from your session?
- What are you going to share that they don't already know?

Have others review your proposal

- CFP mentoring. Email program@wicys.org

Your submission not accepted? Try again!

- Look at our proposal as fluid. Revisit it, update it as new info comes your way

One-page Proposal Tip Guide:

https://www.wicys.org/wp-content/uploads/2022/09/Tips-when-Preparing-a-Conference-Proposal-2-1-2.pdf

women in cybersecurity WiCyS SAN DIEGO AFFILIATE

Additional Resources

1. How to WOW Submission Reviewers with a Stellar Proposal by BrightTALK

   Jun 09, 2021 | 60 mins video | Watch video here

2. CFP Workshop Video (Presented by Meghan Jacquot) by Mid-Atlantic Affiliate

   Feb 14, 2022 | 27 mins video | Watch video here

3. WiCyS 2025 Supplementary Information: here

Main website: https://www.wicys.org/events/wicys-2025/call-for-presenter/

Exercise Break - Know Yourself (5-10 mins)

Find a topic that you are familiar and passionate about, has expertise in, or comfortable to speak on

What is your potential **TITLE**? *(hardest to do and you can do it last!)*

- Draft one! Or decide it after you write the abstract and outline
- Need to be a good indication of content of session

What is your potential **ABSTRACT**? *(summarizing what you want to talk about in 250 words)*

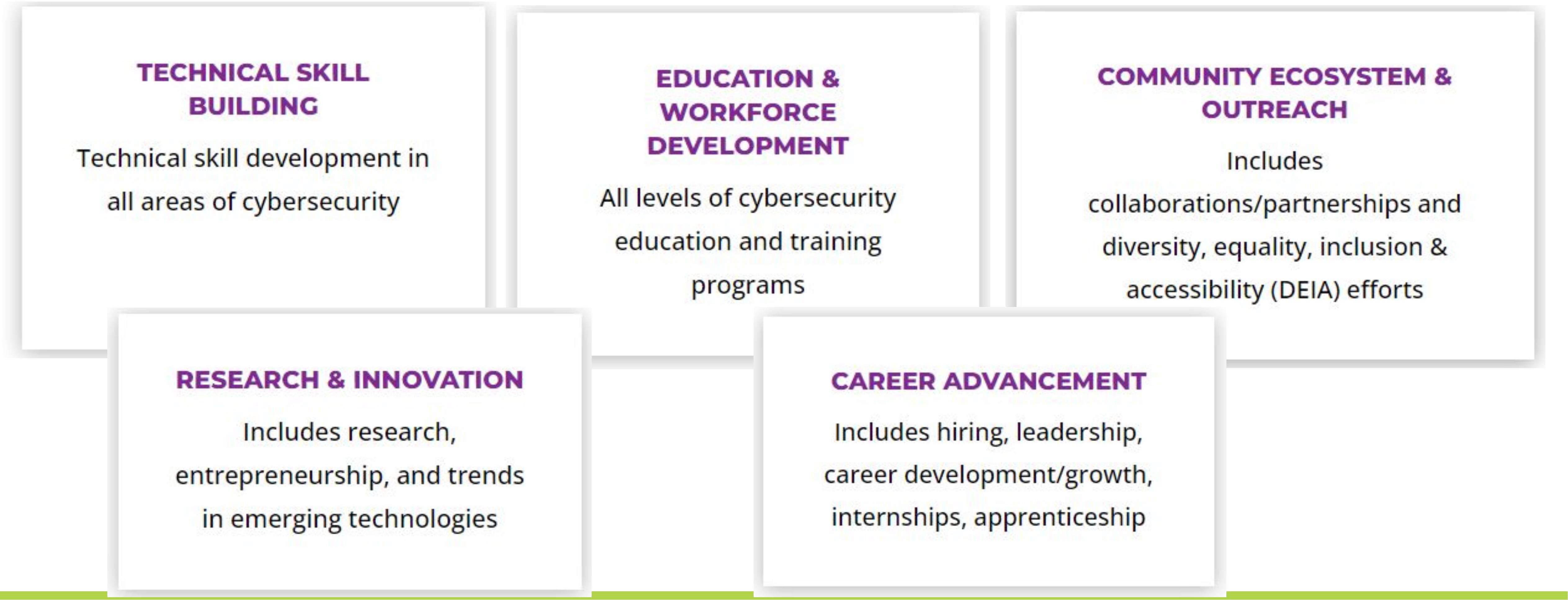
Write a couple of sentences for the abstract

- Need to be precise and best to tell your unique story

What is your potential **OUTLINE**? *(probably easiest out of the three and you can do it first!)*

- Write 3 to 5 bullet points for the outline
- Additional info and what audience can learn from your session

How does your topic fit into the tracks?



TECHNICAL SKILL BUILDING

Technical skill development in all areas of cybersecurity

EDUCATION & WORKFORCE DEVELOPMENT

All levels of cybersecurity education and training programs

COMMUNITY ECOSYSTEM & OUTREACH

Includes collaborations/partnerships and diversity, equality, inclusion & accessibility (DEIA) efforts

RESEARCH & INNOVATION

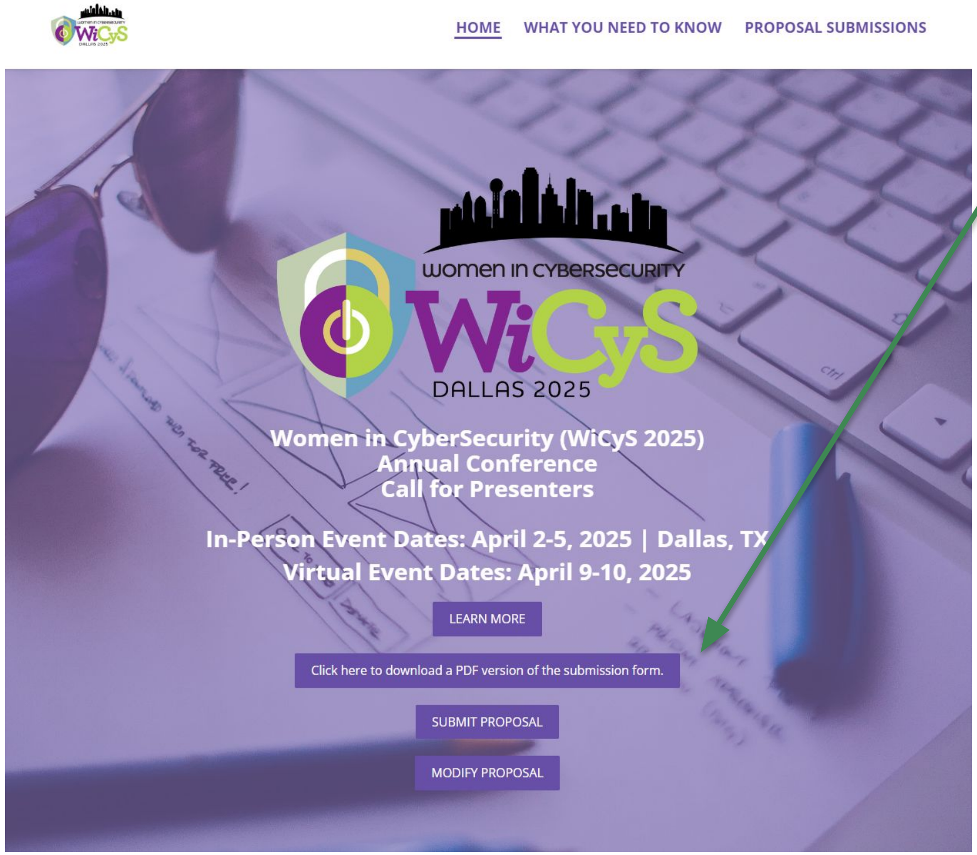
Includes research, entrepreneurship, and trends in emerging technologies

CAREER ADVANCEMENT

Includes hiring, leadership, career development/growth, internships, apprenticeship

Submission Link:

https://www.eventstimes10as.com/WiCyS-CFP25



Women in CyberSecurity (WiCyS 2025)
Annual Conference
Call for Presenters

In-Person Event Dates: April 2-5, 2025 | Dallas, TX
Virtual Event Dates: April 9-10, 2025

You can now download a PDF version of the submission form first before submitting online.

See Submission form questions **HERE**
(3 pages)

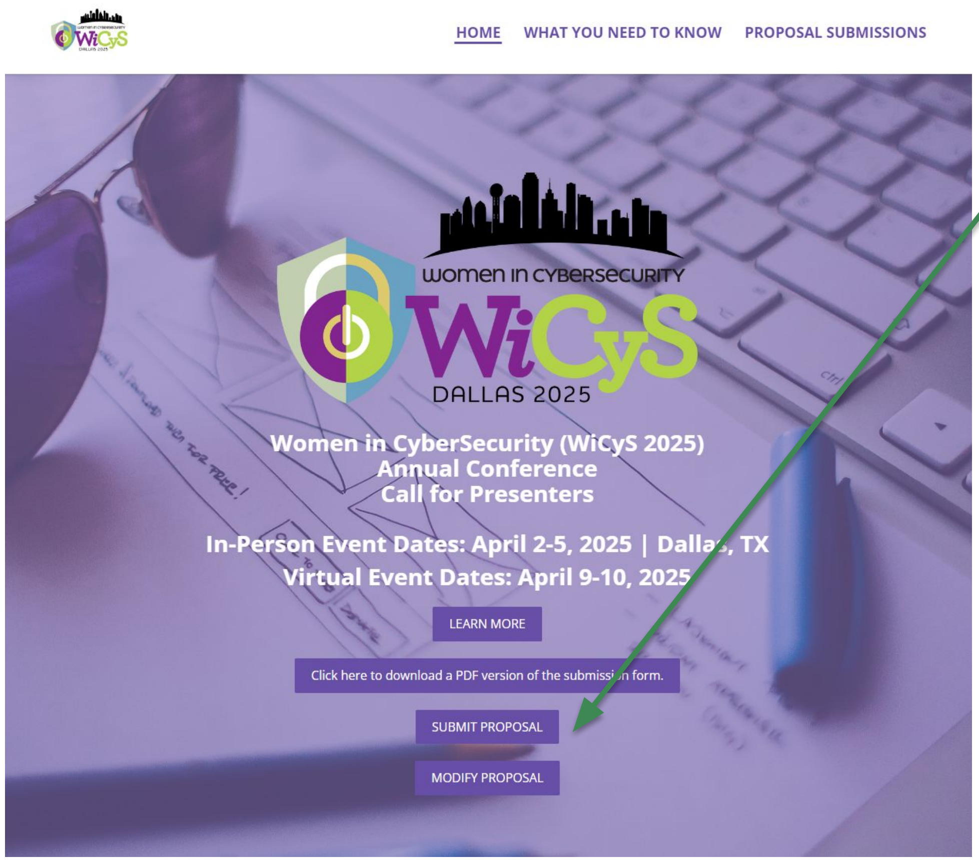
Example questions:

- Has this session content been presented at any public event before?
- Which attendees could benefit from this session?
  -Beginner/early career (0-5 yrs),
  -Mid career (6-10 yrs)
  -Senior (10+ yrs)
- What is the attendee's expected take-away from the session?

Tips: print out or read submission form questions beforehand.
DO NOT WAIT TILL THE LAST DAY (Nov 4) TO SUBMIT.

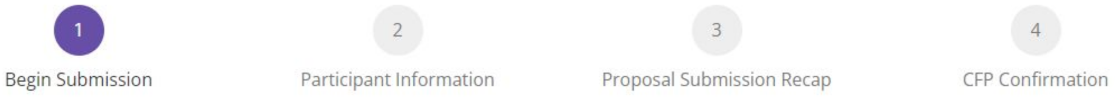
Submission Link:

https://www.eventstimes10as.com/WiCyS-CFP25



Women in CyberSecurity (WiCyS 2025)
Annual Conference
Call for Presenters

In-Person Event Dates: April 2-5, 2025 | Dallas, TX
Virtual Event Dates: April 9-10, 2025



Submitter's info

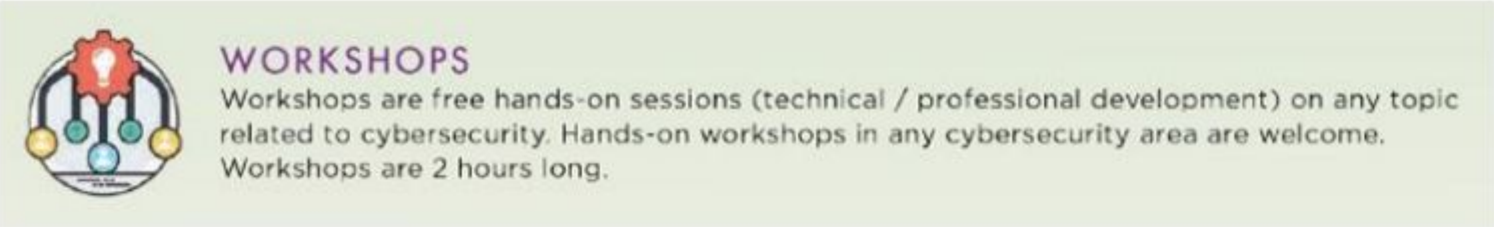
Submission info:

- Title
- Tracks
- Presented before
- Which attendees could benefit
- Required to have previous cybersecurity skill
- Addressing what problem
- Solution presented in 1-2 sentences
- Intended attendee/type for this session
- Involve attendee participation
- Fulfilling WiCyS’s mission
- Abstract
- Outline
- Create password for modify proposal later

Questions?

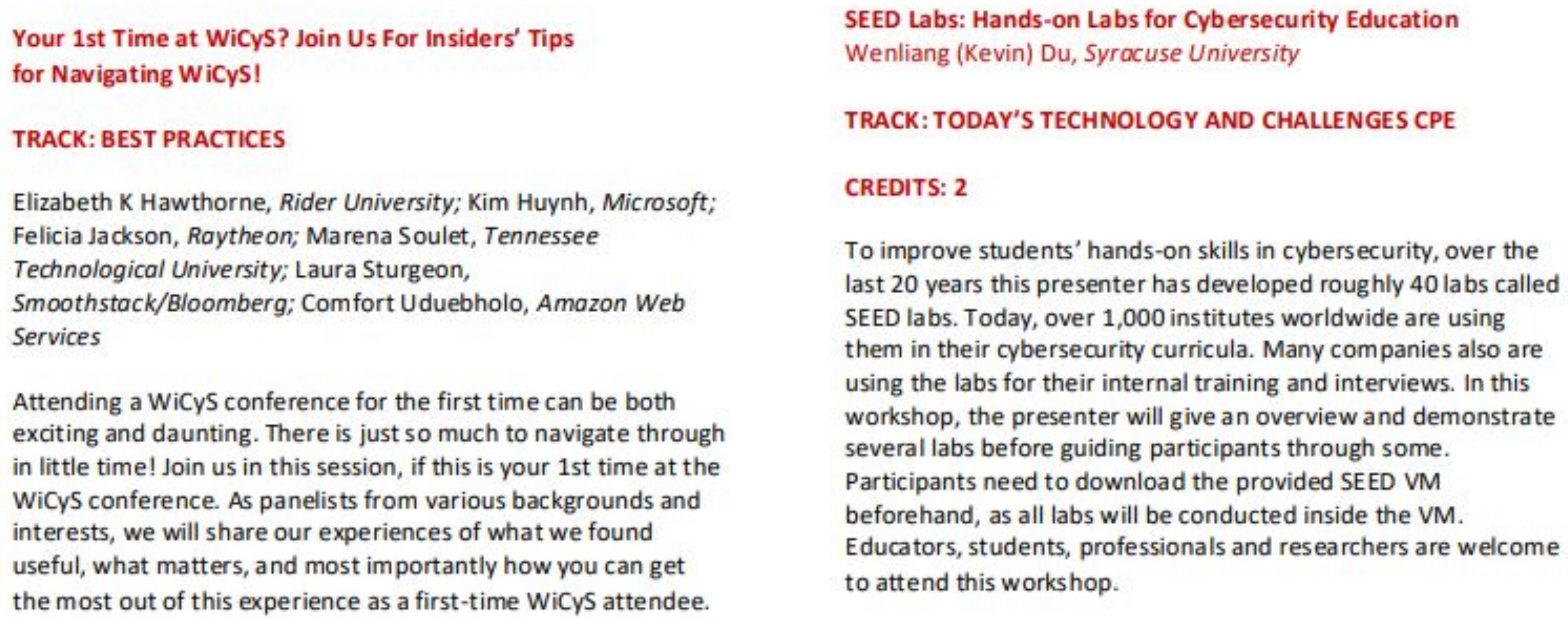
Examples

Example 1.1



WORKSHOPS

Workshops are free hands-on sessions (technical / professional development) on any topic related to cybersecurity. Hands-on workshops in any cybersecurity area are welcome. Workshops are 2 hours long.



Your 1st Time at WiCyS? Join Us For Insiders' Tips for Navigating WiCyS!

TRACK: BEST PRACTICES

Elizabeth K Hawthorne, *Rider University;* Kim Huynh, *Microsoft;* Felicia Jackson, *Raytheon;* Marena Soulet, *Tennessee Technological University;* Laura Sturgeon, *Smoothstack/Bloomberg;* Comfort Uduebholo, *Amazon Web Services*

Attending a WiCyS conference for the first time can be both exciting and daunting. There is just so much to navigate through in little time! Join us in this session, if this is your 1st time at the WiCyS conference. As panelists from various backgrounds and interests, we will share our experiences of what we found useful, what matters, and most importantly how you can get the most out of this experience as a first-time WiCyS attendee.

SEED Labs: Hands-on Labs for Cybersecurity Education

Wenliang (Kevin) Du, *Syracuse University*

TRACK: TODAY'S TECHNOLOGY AND CHALLENGES CPE

CREDITS: 2

To improve students' hands-on skills in cybersecurity, over the last 20 years this presenter has developed roughly 40 labs called SEED labs. Today, over 1,000 institutes worldwide are using them in their cybersecurity curricula. Many companies also are using the labs for their internal training and interviews. In this workshop, the presenter will give an overview and demonstrate several labs before guiding participants through some. Participants need to download the provided SEED VM beforehand, as all labs will be conducted inside the VM. Educators, students, professionals and researchers are welcome to attend this workshop.

Example 1.2-Workshop

2023--Let’s Get Logic(al): A Crash Course on Building Security Detections
Alexis Merritt and Holly Parrish Syed

Ever wonder how security products catch adversarial activity? That’s a combination of several security roles, such as security developers, threat intelligence analysts and threat hunters coming together to create security detections that are escalated for further attention from security operations. During this interactive workshop, participants will receive a crash course on security detection engineering from basic concepts to an opportunity to write their own detections. Participants will uncover the basics of detection engineering from understanding types such as signature and behavior based detections. Then, participants will be introduced to standardized formats to expand their own capabilities to apply their knowledge in various ways from certifications to conversations with industry peers. With the basics explained, the workshop will move to a high-level overview of methods to gather use cases from available threat intelligence and data sources. Next, the importance of testing and revisiting (tuning!) their detections in an organization’s production environment will be discussed. Testing security detections provides an opportunity for an organization to confirm detections are production ready and will not break existing workflows. Participants will share their experiences with noise to signal ratios to kick off the tuning section of the workshop. Finally, everyone will have an opportunity to review an incident report and create their own security detections in a group setting. The workshop will conclude with the groups sharing and learning from each other’s security detection examples. Participants will leave with their notes, conversations and the speaker-provided materials to apply to their day-to-day security detection toolkit.

Example 1.3-Workshop

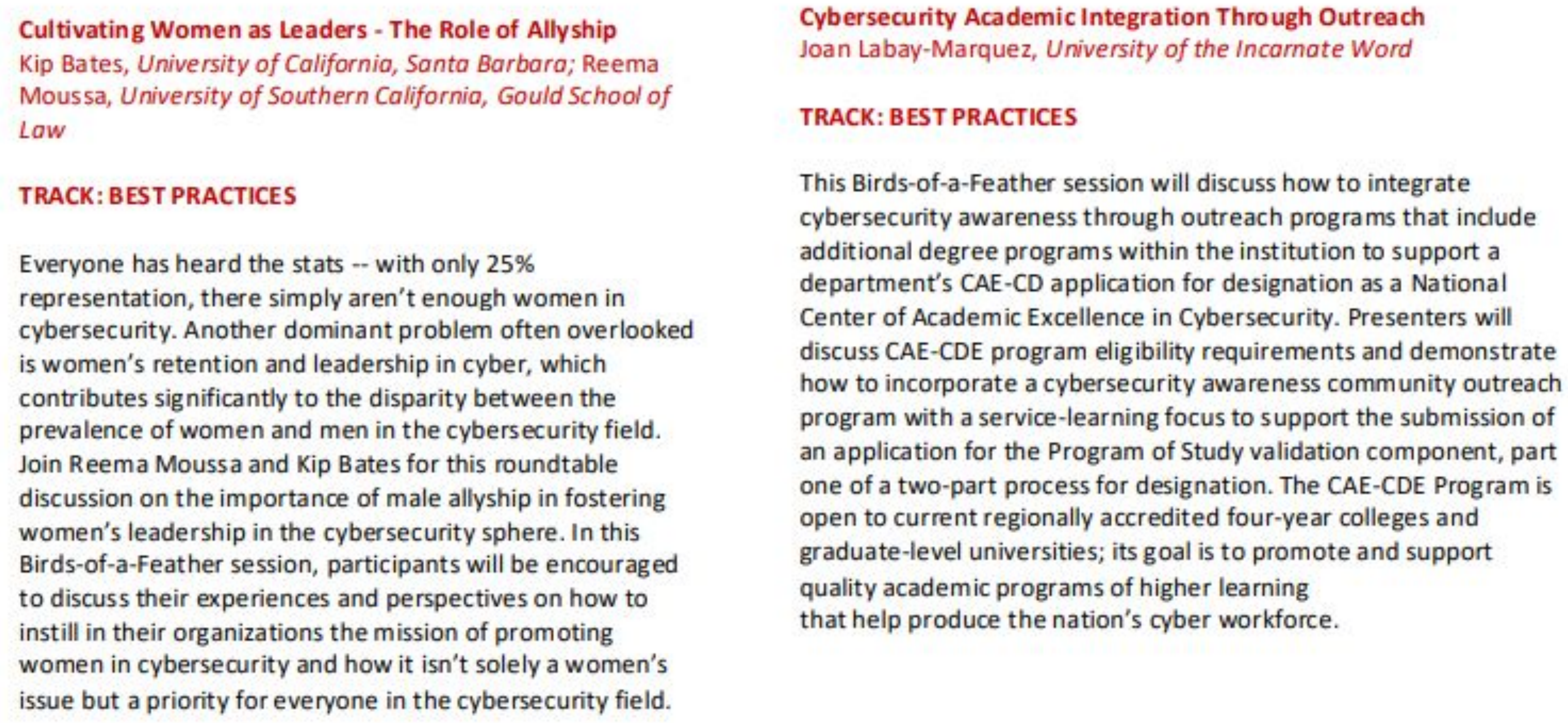
2022--Create Confidence When it Matters to Take Your Career to the Next Level
Micha Goebig, Go Big Coaching; Katrina Zidel, Kreating Boldly, Inc.
TRACK: CAREER DEVELOPMENT

It can be challenging to be seen and heard as a female professional in a male-dominated sphere like cybersecurity and exude an air of confidence when it matters. These days, visibility and confidence seem to be about as vital to taking a career to the next level as expertise and experience. In this workshop, confidence and leadership coach, Micha Goebig, will bust a few misconceptions about confidence and share practices and tools to help attendees step up their authentic visibility and confidence presence. This is for any attendees who are done not feeling seen or heard in the professional environment; who are ready to exchange the sense of not belonging for owning their uniqueness; who want to learn to show up authentically and create safety through self-trust; and need input and strategies to tap into their full potential in their career and life.

Example 2.1

BIRDS OF A FEATHER (BoaF)

Birds of a Feather are informal discussion sessions on just about any topic related to cybersecurity, that elicit participant discussions. These sessions can be a great way to share ideas and be introduced to current issues or trends. BoaF sessions are 45 minutes long.



Cultivating Women as Leaders - The Role of Allyship

Kip Bates, *University of California, Santa Barbara;* Reema Moussa, *University of Southern California, Gould School of Law*

TRACK: BEST PRACTICES

Everyone has heard the stats -- with only 25% representation, there simply aren't enough women in cybersecurity. Another dominant problem often overlooked is women's retention and leadership in cyber, which contributes significantly to the disparity between the prevalence of women and men in the cybersecurity field. Join Reema Moussa and Kip Bates for this roundtable discussion on the importance of male allyship in fostering women's leadership in the cybersecurity sphere. In this Birds-of-a-Feather session, participants will be encouraged to discuss their experiences and perspectives on how to instill in their organizations the mission of promoting women in cybersecurity and how it isn't solely a women's issue but a priority for everyone in the cybersecurity field.

Cybersecurity Academic Integration Through Outreach

Joan Labay-Marquez, *University of the Incarnate Word*

TRACK: BEST PRACTICES

This Birds-of-a-Feather session will discuss how to integrate cybersecurity awareness through outreach programs that include additional degree programs within the institution to support a department's CAE-CD application for designation as a National Center of Academic Excellence in Cybersecurity. Presenters will discuss CAE-CDE program eligibility requirements and demonstrate how to incorporate a cybersecurity awareness community outreach program with a service-learning focus to support the submission of an application for the Program of Study validation component, part one of a two-part process for designation. The CAE-CDE Program is open to current regionally accredited four-year colleges and graduate-level universities; its goal is to promote and support quality academic programs of higher learning that help produce the nation's cyber workforce.

Example 2.2-BoaF

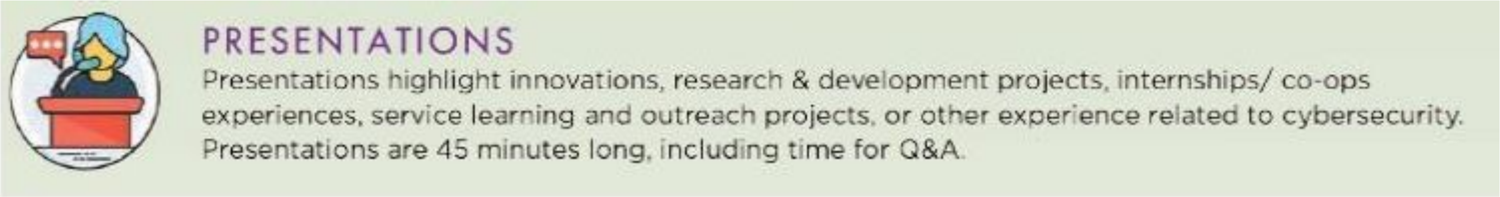
2023--Navigating the Infosec World with Physical and Mental Illness
Elaine Harrison-Neukirch

Many people have a chronic illness and/or chronic pain. They may hide this from teammates to not appear inadequate or weak. Not only are people juggling work and family but also the many symptoms that accompany chronic illness. Depending on a person's position, they may be working long hours or have a stressful job. There are a multitude of factors that can increase pain, fatigue and other chronic illness symptoms. Chronic illness can lead to imposter syndrome, particularly if someone is working in a toxic environment or work culture. Having to constantly prove themselves leads to more stress which, in turn, can cause symptoms to increase. This discussion is focused on strategies used to keep chronic illness symptoms at bay when under a lot of stress, deadlines, etc.

2022--Why Are There so Many aaS(es) in the Cloud?
Atia Ibrahim, Optum
TRACK: TODAY'S TECHNOLOGY AND CHALLENGES

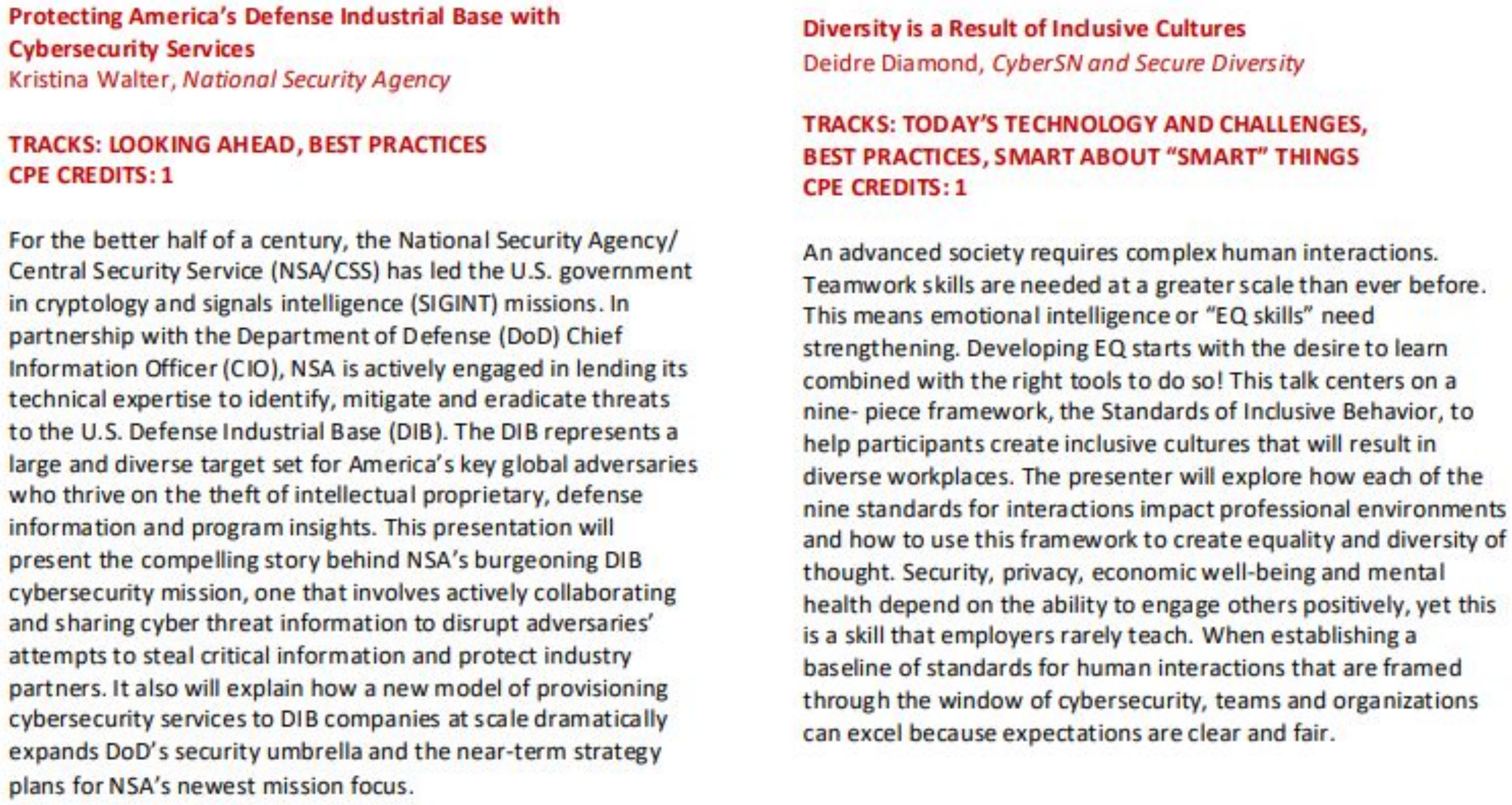
Cloud technology is everywhere and on everyone's mind. The presenter decided to get into the cloud only five years ago. In that short period of time, the cloud has changed its shapes, and the pandemic helped it grow into cumulonimbus. The presenter had to change their 20 years of data center security mindset and use experience to support a current position as cloud security architect. This session will help remove some common mysteries and fears about cloud and help beginners in cybersecurity get a better understanding of cloud security. Discussions will revolve around how cloud security is different than data center security, why things in the cloud have aaS (as a Service) attached to them, and how aaS(es) play a role in cloud security. Examples will be provided on aaS(es) that impact daily lives. Netflix – is it a SaaS or PaaS? Conversation will be encouraged to remove the mystery about the cloud and cloud security.

Example 3.1



PRESENTATIONS

Presentations highlight innovations, research & development projects, internships/ co-ops experiences, service learning and outreach projects, or other experience related to cybersecurity. Presentations are 45 minutes long, including time for Q&A.



Protecting America's Defense Industrial Base with Cybersecurity Services

Kristina Walter, *National Security Agency*

TRACKS: LOOKING AHEAD, BEST PRACTICES
CPE CREDITS: 1

For the better half of a century, the National Security Agency/ Central Security Service (NSA/CSS) has led the U.S. government in cryptology and signals intelligence (SIGINT) missions. In partnership with the Department of Defense (DoD) Chief Information Officer (CIO), NSA is actively engaged in lending its technical expertise to identify, mitigate and eradicate threats to the U.S. Defense Industrial Base (DIB). The DIB represents a large and diverse target set for America's key global adversaries who thrive on the theft of intellectual proprietary, defense information and program insights. This presentation will present the compelling story behind NSA's burgeoning DIB cybersecurity mission, one that involves actively collaborating and sharing cyber threat information to disrupt adversaries' attempts to steal critical information and protect industry partners. It also will explain how a new model of provisioning cybersecurity services to DIB companies at scale dramatically expands DoD's security umbrella and the near-term strategy plans for NSA's newest mission focus.

Diversity is a Result of Inclusive Cultures

Deidre Diamond, *CyberSN and Secure Diversity*

TRACKS: TODAY'S TECHNOLOGY AND CHALLENGES, BEST PRACTICES, SMART ABOUT "SMART" THINGS
CPE CREDITS: 1

An advanced society requires complex human interactions. Teamwork skills are needed at a greater scale than ever before. This means emotional intelligence or "EQ skills" need strengthening. Developing EQ starts with the desire to learn combined with the right tools to do so! This talk centers on a nine- piece framework, the Standards of Inclusive Behavior, to help participants create inclusive cultures that will result in diverse workplaces. The presenter will explore how each of the nine standards for interactions impact professional environments and how to use this framework to create equality and diversity of thought. Security, privacy, economic well-being and mental health depend on the ability to engage others positively, yet this is a skill that employers rarely teach. When establishing a baseline of standards for human interactions that are framed through the window of cybersecurity, teams and organizations can excel because expectations are clear and fair.

Example 3.2--Presentation

2023--Just a Shift to the Left
Diane Stephens and Hanan Hibshi

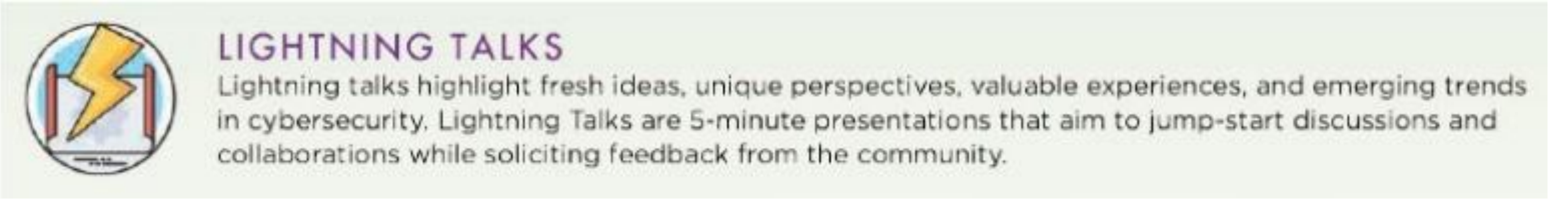
How do companies harden their source code and tighten up their processes to prevent exploitation? Securing applications starts by shifting security left to the start or the beginning of the development lifecycle. Research suggests that as much as 75% of security vulnerabilities are the result of coding errors. Testing and patching at the end of the development cycle leave organizations and critical infrastructure open to unnecessary risks and costs. With just a shift to the left, companies can educate developers, eliminate vulnerabilities and protect valuable resources and assets. The goal of this talk is to explain how vulnerabilities are introduced and suggest secure coding best practices. The presenters will explain common programming errors in C and C++ and describe how these errors can lead to code that is vulnerable to exploitation. They will highlight key aspects of C and C++ that make the two languages vulnerable and why programmers continue to adopt insecure coding practices. After review of secure programming practices, they will review the Rust programming language, a new memory-safe language gaining momentum in the industry. Rust is based on the following three tenets: safety, speed and fearless concurrency. They will analyze what makes it a compelling alternative to C as well as the hurdles to writing in it, such as its complex ownership and lifetime rules. They will consider why even getting a simple Rust program to compile can be frustrating and work to make sense of the oddities of Rust, demonstrate a new visualization development tool, and assess what a transition to this language might look like.

Example 3.3--Presentation

2022-Trapped in the Wolf Den: A Dive into Compromises From Within the Walls of a SOC
Lisa Tetrault and Samantha Van Aaken, Arctic Wolf
TRACK: BEST PRACTICES

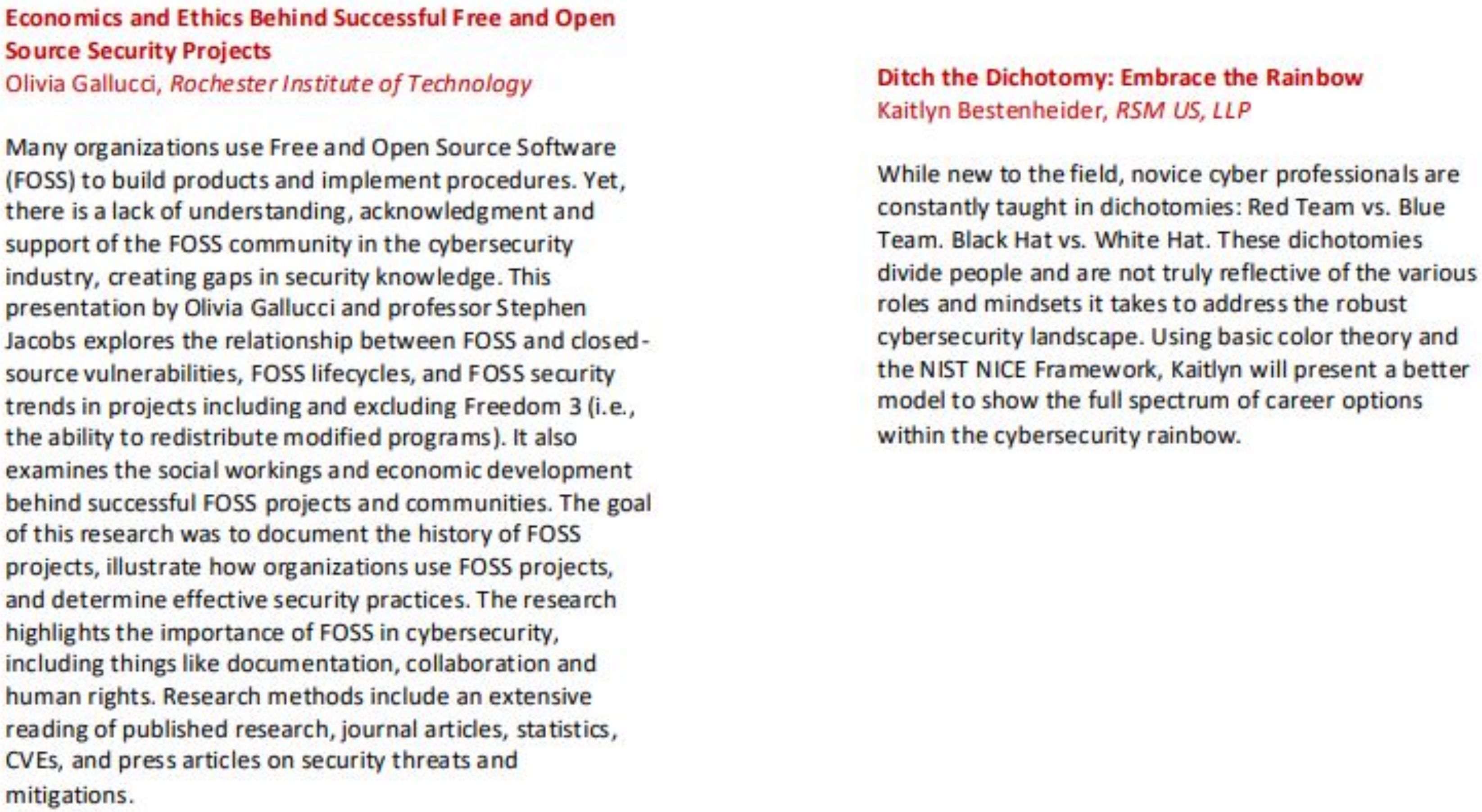
When it comes to mitigating the impact of any security incident, it’s a race against time to ensure the safety of a team’s most valuable assets. Organizations rely on email to conduct business, communicate, share information and set daily meetings. Email account compromise is an unsettlingly common method of attack for bad actors and can have a huge impact on business. Business email compromise attacks have already cost U.S. businesses at least $1.6 billion in losses from 2013 to today. According to the Federal Bureau of Investigation, that number could easily be as high as $5.3 billion around the world. This presentation will explore real-world examples when there is an attack starting from the detection triage boards. In this interactive session, a team of security operations experts will walk through what detection alerts they see leading up to and during different types of compromises. They will showcase the initial detections, incident response process, remediation steps, and best practices that could have mitigated various forms of common attacks. Participants will get a front-row seat into a thrilling day in the life of an SOC Analyst. Welcome to the den of wolves. They’ve been waiting for you.

Example 4.1



LIGHTNING TALKS

Lightning talks highlight fresh ideas, unique perspectives, valuable experiences, and emerging trends in cybersecurity. Lightning Talks are 5-minute presentations that aim to jump-start discussions and collaborations while soliciting feedback from the community.



Economics and Ethics Behind Successful Free and Open Source Security Projects
Olivia Gallucci, *Rochester Institute of Technology*

Many organizations use Free and Open Source Software (FOSS) to build products and implement procedures. Yet, there is a lack of understanding, acknowledgment and support of the FOSS community in the cybersecurity industry, creating gaps in security knowledge. This presentation by Olivia Gallucci and professor Stephen Jacobs explores the relationship between FOSS and closed-source vulnerabilities, FOSS lifecycles, and FOSS security trends in projects including and excluding Freedom 3 (i.e., the ability to redistribute modified programs). It also examines the social workings and economic development behind successful FOSS projects and communities. The goal of this research was to document the history of FOSS projects, illustrate how organizations use FOSS projects, and determine effective security practices. The research highlights the importance of FOSS in cybersecurity, including things like documentation, collaboration and human rights. Research methods include an extensive reading of published research, journal articles, statistics, CVEs, and press articles on security threats and mitigations.

Ditch the Dichotomy: Embrace the Rainbow
Kaitlyn Bestenheider, *RSM US, LLP*

While new to the field, novice cyber professionals are constantly taught in dichotomies: Red Team vs. Blue Team. Black Hat vs. White Hat. These dichotomies divide people and are not truly reflective of the various roles and mindsets it takes to address the robust cybersecurity landscape. Using basic color theory and the NIST NICE Framework, Kaitlyn will present a better model to show the full spectrum of career options within the cybersecurity rainbow.

Example 4.2—Lightning Talk

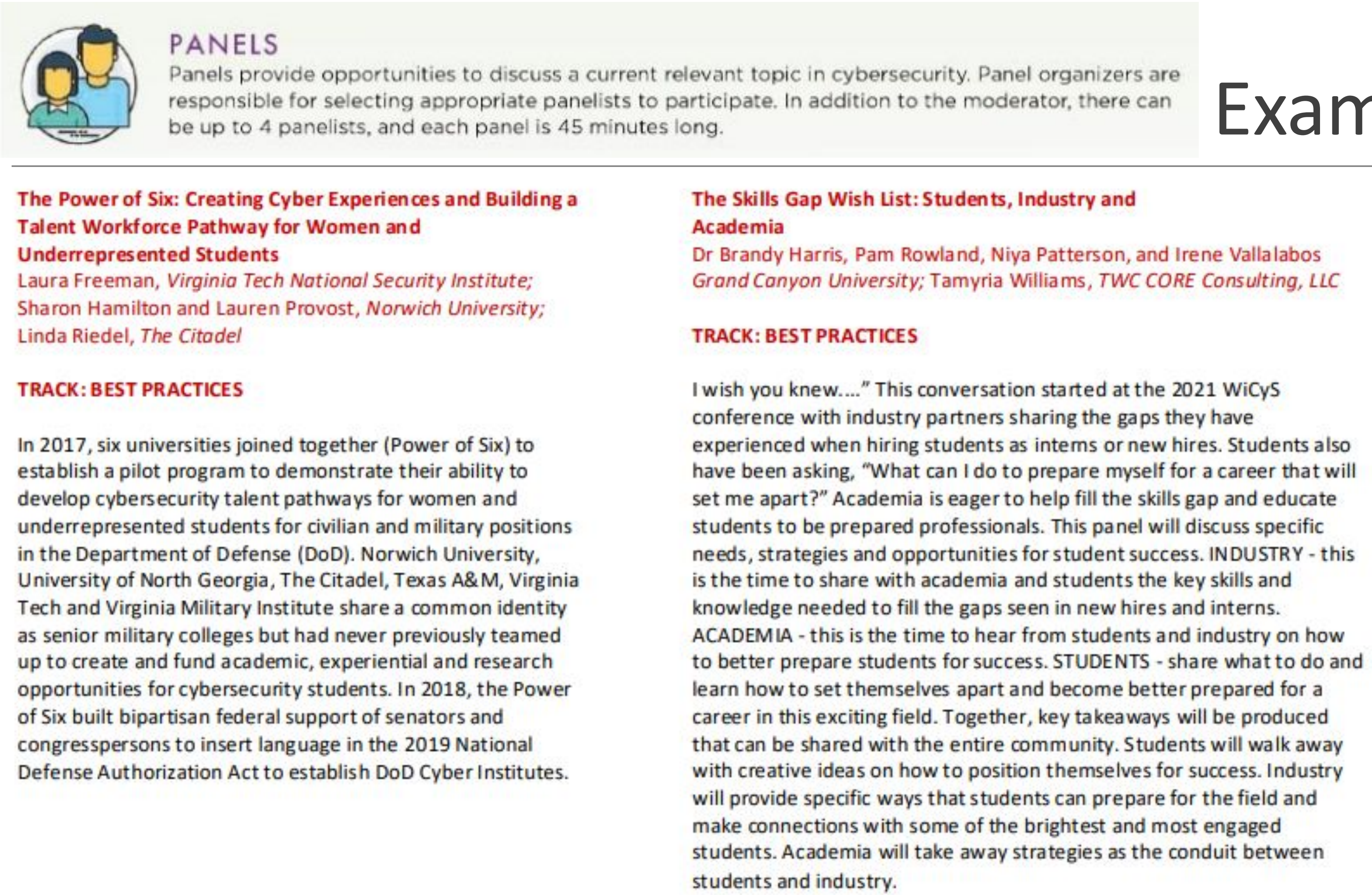
2023--Great Student, Great Employee: How to Thrive During the Post-Grad Transition
Molly Soja

Students have had a syllabus to follow, deadlines to meet and a group of comrades in the same situation for the last few years. Moving into the workforce with different expectations and structure can be daunting at first, but this session is designed to prepare students for what comes next. Learn how best to set up for success with advice on networking, choosing a career path, finding mentors, asking the scary questions and maintaining a work-life balance.

2022--Ditch the Dichotomy: Embrace the Rainbow
Kaitlyn Bestenheider, RSM US, LLP

While new to the field, novice cyber professionals are constantly taught in dichotomies: Red Team vs. Blue Team. Black Hat vs. White Hat. These dichotomies divide people and are not truly reflective of the various roles and mindsets it takes to address the robust cybersecurity landscape. Using basic color theory and the NIST NICE Framework, Kaitlyn will present a better model to show the full spectrum of career options within the cybersecurity rainbow.

Example 5.1



PANELS

Panels provide opportunities to discuss a current relevant topic in cybersecurity. Panel organizers are responsible for selecting appropriate panelists to participate. In addition to the moderator, there can be up to 4 panelists, and each panel is 45 minutes long.

The Power of Six: Creating Cyber Experiences and Building a Talent Workforce Pathway for Women and Underrepresented Students

Laura Freeman, *Virginia Tech National Security Institute;*
Sharon Hamilton and Lauren Provost, *Norwich University;*
Linda Riedel, *The Citadel*

TRACK: BEST PRACTICES

In 2017, six universities joined together (Power of Six) to establish a pilot program to demonstrate their ability to develop cybersecurity talent pathways for women and underrepresented students for civilian and military positions in the Department of Defense (DoD). Norwich University, University of North Georgia, The Citadel, Texas A&M, Virginia Tech and Virginia Military Institute share a common identity as senior military colleges but had never previously teamed up to create and fund academic, experiential and research opportunities for cybersecurity students. In 2018, the Power of Six built bipartisan federal support of senators and congresspersons to insert language in the 2019 National Defense Authorization Act to establish DoD Cyber Institutes.

The Skills Gap Wish List: Students, Industry and Academia

Dr Brandy Harris, Pam Rowland, Niya Patterson, and Irene Vallalabos
Grand Canyon University; Tamyria Williams, *TWC CORE Consulting, LLC*

TRACK: BEST PRACTICES

I wish you knew...." This conversation started at the 2021 WiCyS conference with industry partners sharing the gaps they have experienced when hiring students as interns or new hires. Students also have been asking, "What can I do to prepare myself for a career that will set me apart?" Academia is eager to help fill the skills gap and educate students to be prepared professionals. This panel will discuss specific needs, strategies and opportunities for student success. INDUSTRY - this is the time to share with academia and students the key skills and knowledge needed to fill the gaps seen in new hires and interns. ACADEMIA - this is the time to hear from students and industry on how to better prepare students for success. STUDENTS - share what to do and learn how to set themselves apart and become better prepared for a career in this exciting field. Together, key takeaways will be produced that can be shared with the entire community. Students will walk away with creative ideas on how to position themselves for success. Industry will provide specific ways that students can prepare for the field and make connections with some of the brightest and most engaged students. Academia will take away strategies as the conduit between students and industry.

Example 5.2--Panel

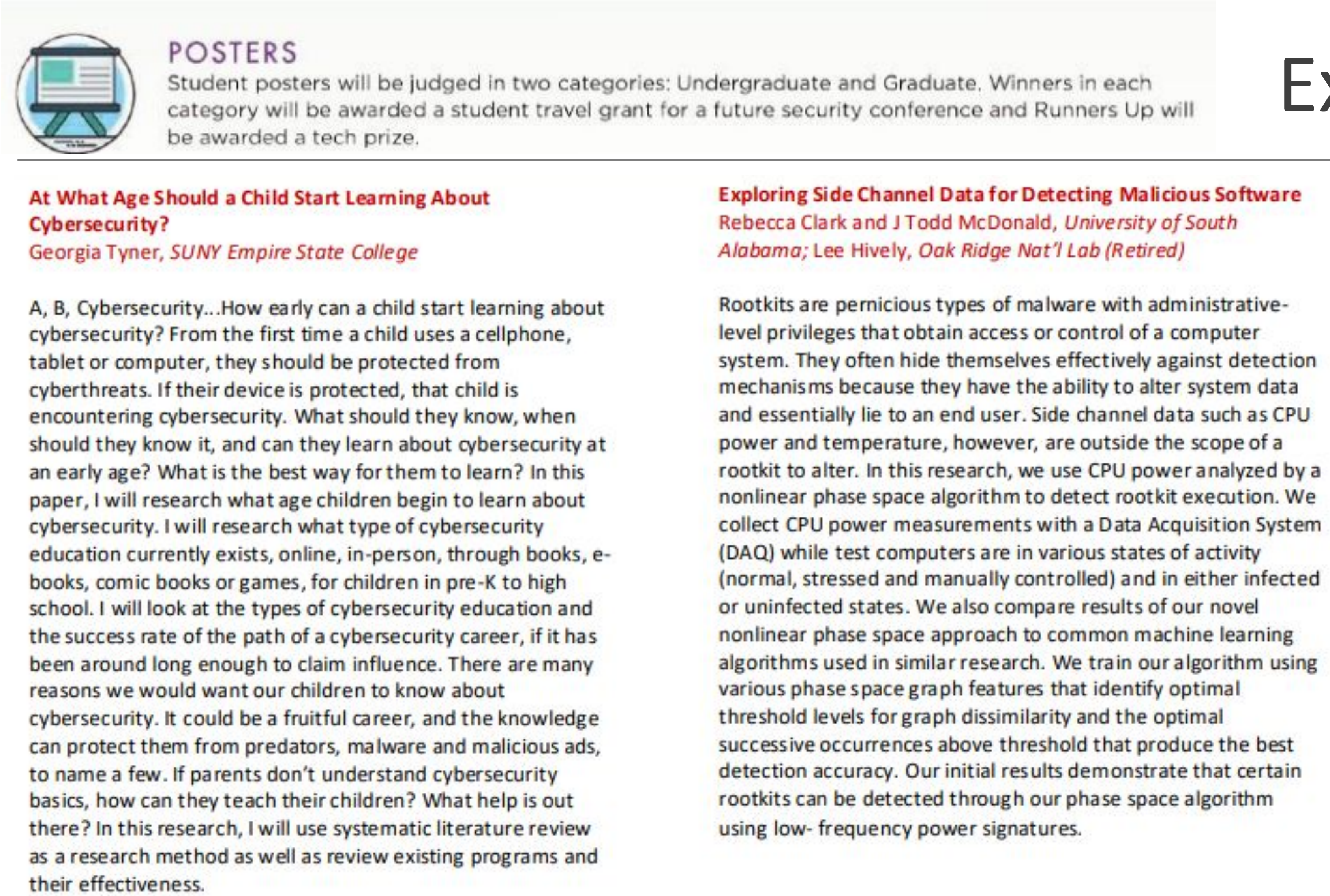
2023--CyberCrime Prevention and Investigation: A Case Study of Public, Private and University Partnership
Katie Shuck, Ashley Podhradsky, Arica Kulm and Kendra Russell

The DigForCE Lab, Digital Forensics for Cyber Enforcement, at Dakota State University (DSU) has developed public, private and educational partnerships to help prevent and investigate cybercrime in South Dakota. In this panel, the directors of the DigForCE Lab, the cyberintelligence analyst in the South Dakota Fusion Center, moderated by the vice president of Research at DSU, will discuss how the lab was created, its funding model, initial challenges and strengths it brings to the state of South Dakota.

2022--You've Got This: Stories of Career Pivots and How to Successfully Start a Cyber Career
Jennifer Bate, Deloitte; Jennifer Cheung, NWIC Pacific; Meghan Jacquot, Recorded Future; Ashley Richardson Sequeira, Palo Alto Networks; Alma Maria Rinasz, Bug Bounty Services
TRACK: CAREER DEVELOPMENT

A panel of four women, none of whom started in cybersecurity, who successfully pivoted to the industry will be moderated by another cyber professional who has a story to share after a long career gap and return to the field. Emphasis and care were given to put together a diverse panel with a variety of backgrounds, experiences and belief in #ShareTheMic. Two panelists are veterans and two are BIPOC. Each panelist has her own story, but they have common threads of collaboration, curiosity and determination. Questions will be carefully crafted to deliver a nuanced perspective to the audience. The hope is that conference attendees have takeaways regarding representation (they can see themselves in the panel) as well as concrete ideas for how to pivot (if applicable), start in cyber and be successful in the industry. The panel will end with a question and answer session as well as networking to get to know the panelists. All panelists are involved in WiCyS and encourage women in tech and cybersecurity, so part of the panel's focus will be to encourage attendees that they can be successful wherever they are in their journey

Example 6.1



POSTERS

Student posters will be judged in two categories: Undergraduate and Graduate. Winners in each category will be awarded a student travel grant for a future security conference and Runners Up will be awarded a tech prize.

At What Age Should a Child Start Learning About Cybersecurity?

Georgia Tyner, *SUNY Empire State College*

A, B, Cybersecurity...How early can a child start learning about cybersecurity? From the first time a child uses a cellphone, tablet or computer, they should be protected from cyberthreats. If their device is protected, that child is encountering cybersecurity. What should they know, when should they know it, and can they learn about cybersecurity at an early age? What is the best way for them to learn? In this paper, I will research what age children begin to learn about cybersecurity. I will research what type of cybersecurity education currently exists, online, in-person, through books, e-books, comic books or games, for children in pre-K to high school. I will look at the types of cybersecurity education and the success rate of the path of a cybersecurity career, if it has been around long enough to claim influence. There are many reasons we would want our children to know about cybersecurity. It could be a fruitful career, and the knowledge can protect them from predators, malware and malicious ads, to name a few. If parents don't understand cybersecurity basics, how can they teach their children? What help is out there? In this research, I will use systematic literature review as a research method as well as review existing programs and their effectiveness.

Exploring Side Channel Data for Detecting Malicious Software

Rebecca Clark and J Todd McDonald, *University of South Alabama;* Lee Hively, *Oak Ridge Nat'l Lab (Retired)*

Rootkits are pernicious types of malware with administrative-level privileges that obtain access or control of a computer system. They often hide themselves effectively against detection mechanisms because they have the ability to alter system data and essentially lie to an end user. Side channel data such as CPU power and temperature, however, are outside the scope of a rootkit to alter. In this research, we use CPU power analyzed by a nonlinear phase space algorithm to detect rootkit execution. We collect CPU power measurements with a Data Acquisition System (DAQ) while test computers are in various states of activity (normal, stressed and manually controlled) and in either infected or uninfected states. We also compare results of our novel nonlinear phase space approach to common machine learning algorithms used in similar research. We train our algorithm using various phase space graph features that identify optimal threshold levels for graph dissimilarity and the optimal successive occurrences above threshold that produce the best detection accuracy. Our initial results demonstrate that certain rootkits can be detected through our phase space algorithm using low- frequency power signatures.

Example 6.2—Student Poster

2023--Machine-Learning Techniques to Design an Intrusion Detection System in Computer Networks
Sara Yavari; DePaul University and Seyed Mohammad Mosavi; Iran University of Science and Technology (IUST)

Computer networks are faced with a huge amount of data to analyze. Investigation of attacks on them shows that each type of cyberattack has certain characteristics as does the data set of intrusion detection systems. Therefore, knowing the set of optimal features for each type of attack is a suitable solution for detecting the attack pattern because the intrusion detection system will be able to use only the set of features appropriate to that attack to detect each type. For this purpose, a method is presented that is able to meet all the above requirements and show the relationship between the features for their better analysis. In this research, the problem of intrusion detection is raised as a supervision problem. The KDD99 dataset was used to train and test this model. In this research, k-nearest neighbor (KNN) algorithm and Recurrent Neural Networks (RNNs), which is a type of supervised deep learning, are used.

2022--U.S. Ransomware Analysis of Public Sector Infrastructure
Tahlla Taylor, University of Texas Dallas

Ransomware has been emerging as one of the leading threats in cybersecurity. Every year, hackers become more creative, and their targets remain unsuspecting. Over several years, hospitals, police stations, schools and other objects of public sector infrastructure have experienced an increase in attacks across the U.S. I present an exploratory analysis of over 1,800 ransomware cases in the U.S. from 2016 through the present. I classify these attacks according to their targets, locations and impact. I show that the severity of attacks range from no change in the organization (very low) to life-threatening (very high) depending on the type of attack and target. My analysis advances our understanding of the strategic considerations underlying this cybercrime, and I will present solutions to reduce ransomware attacks in this sector.