



#WiCyS2023



2023 WICYS CONFERENCE

March 16-18 • Denver, CO

VIP Sponsors

Bloomberg

FORTINET®

Optum

 **Raytheon
Technologies**

We asked for one word to describe your feelings about attending WiCyS 2023...



TABLE OF CONTENTS

• Welcome4
• WiCyS Organization5
• Keynote Speakers6
• Thanks to Sponsors7
• Thanks to Committee Members9
• Track and Session Guide	13
• Schedule at a Glance.	14
• Thursday Agenda	16
• Friday Agenda	19
• Saturday Agenda	23
• Pre-Conference Sessions	27
• Meet-Ups and Chats	28
• Workshop Descriptions	29
• Presentation Descriptions	36
• Birds of a Feather Descriptions	42
• Panel Session Descriptions	45
• Lightning Talk Descriptions	48
• Career Village Talks Descriptions	53
• Student Poster Descriptions	56
• Speaker Index.	67
• Career Fair Booths.	77
• Thank You to Sponsors.	80
• Venue/Room Maps	81

BADGE PICK-UP HOURS

THURSDAY	7:00am - 7:00pm
FRIDAY	7:00am - 6:00pm
SATURDAY	7:00am - 9:00am

USE THE APP

BOOST YOUR EXPERIENCE

Have you explored the WiCyS Conference App? After downloading the Whova app to your mobile device, use the email address associated with your conference registration to sign in. You can browse the agenda, view speakers and sponsors, connect with other attendees, and ask conference-related questions by sending a message to “Ask Organizers *Anything*” in the community section.



Scan the code with your mobile device to download the app.

SOCIAL MEDIA CONTEST

Win FREE registration to WiCyS 2024 by sharing your WiCyS experience!

Post on social media using #WiCyS2023 and share key takeaways from workshops, keynotes, panels, etc. We'd love to see photos/videos of you and your community connecting at the conference too!

How to win:

Best Hashtag User will receive FREE Registration to WiCyS 2024.

Best Instagram Reel will receive FREE Registration to WiCyS 2024.

Two “standout” winners will be chosen each day from any platform to receive a WiCyS Store Gift Card. @WiCySorg will send winners a DM.

Remember to tag @WiCySorg and use the #WiCyS2023 hashtag.

WIFI ACCESS CODE

SSID: 2023wicys • Password: Wicys2023

CONFERENCE PHONE NUMBER

For urgent matters or non-medical emergencies during the conference please call or text:
(615) 281-9867

WELCOME TO THE 10TH ANNUAL WiCyS CONFERENCE

Welcome and congratulations on being part of WiCyS 2023! It is spectacular to see how much our community has grown since the conference was launched in 2014 by Dr. Siraj. We are thrilled to welcome new and returning members as we gather to celebrate the milestones we've hit and prepare for the ones that lay ahead. As you expand your network over the next few days, we hope to help you understand why you belong here and all the ways WiCyS can help you achieve your goals.

We are determined to meet you where you are and do everything within our power to help you establish yourself in a burgeoning career field that needs you - there is a 3.4 million global cybersecurity jobs gap, and you are exactly what our industry needs! It is our mission to help you foster meaningful connections with like-minded peers, mentors and industry leaders who can, and will, provide you with personalized guidance on how you can advance your education and career in cybersecurity.

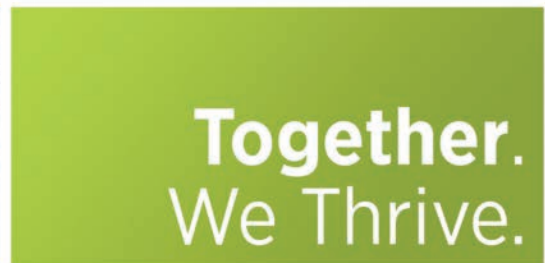
We hope you'll step out of your comfort zone to learn as much as you can over the course of the next three days. We are here to help you reach your fullest potential!

Thank you for coming as you are and for your willingness to learn from and lift each other up. It is you, our members, who are responsible for making WiCyS the dynamic and resilient organization it has become. A special and heartfelt thanks to the hundreds of volunteers that have helped make WiCyS 2023 possible. I can't wait to get to know our incredible WiCyS community over the next few days.

Welcome to the tribe!

Janell Straach

WiCyS Conference Chair and Chair of the Board



CRISIS TEXT
LINE

Text HOME to 741741 from anywhere in the United States, anytime. Crisis Text Line is here for any crisis (24/7). A live, trained Crisis Counselor receives the text and responds, all from our secure online platform. The volunteer Crisis Counselor will help you move from a hot moment to a cool moment.

Additional information can be found here: <https://www.crisistextline.org>

WiCyS ORGANIZATION

BOARD OF DIRECTORS

Dr. Ambareen Siraj

NSF (Siraj is serving in her personal capacity)
Founder, WiCyS

Dr. Janell Straach

Chair of the Board, WiCyS
Faculty, Rice University

Dr. Costis Torgas

Treasurer, WiCyS
Director, Cyber Security and Privacy
Research Institute,
George Washington University

Dr. Dawn M. Beyer

Senior Fellow,
Lockheed Martin Space

Valerie Jane Chua

Tech Campus Manager,
Silicon Valley,
JPMorgan Chase & Co.

Prajakta Jagdale

Director,
Information Security,
Palo Alto Networks

Diana Kelley

Founder and CTO,
SecurityCurve

Marian Merritt

Deputy Director/Lead, Industry
Engagement of the National Initiative
for Cybersecurity Education (NICE),
National Institute of Standards and
Technology (NIST), U.S. Department of
Commerce

Allison Miller

Chief Information Security Officer and
Senior Vice President,
UnitedHealth Group/Optum

Sarah Morales

Senior Program Manager,
Privacy, Safety & Security Engineering,
Google

Noureen Njoroge

Director of Global Cyber Threat
Intelligence,
Nike, Inc.

Dr. Greg Shannon

Chief Cybersecurity Scientist, Idaho
National Laboratory and Chief Science
Officer,
Cybersecurity Manufacturing Innovation
Institute

STAFF

Lynn Dohm

Executive Director

Peter Baldwin

vCFO - Chief Financial Officer

Morgan Garland

Operational Manager

Colleen Huber

Marketing Coordinator

Jaclyn Justice

Professional Affiliate Manager

Quiana Oates

Program Manager

Lana Richardson

Retail Store Management & Executive Assistant to the
Conference Chair

Jessica Robinson

vCISO - Chief Information Security Officer

Myriam Saint Jean

Financial Manager

Laura Villalobos

Community Manager

Maddie Witt

Social Media Specialist & Content Creator

SENIOR ADVISORS

Mary Jane Partain

Director,
Living Learning Communities,
UT Dallas

Michele Tomasic

Director of Operations,
Carnegie Mellon University Software Engineering Institute

2023 WiCyS CONFERENCE

KEYNOTE SPEAKERS

**Fortinet Keynote: Sylvia Schlaphof**

Head of Engineering / Member of the Executive Board, Boll Engineering AG

"Women in Cybersecurity: Creating Magic in Your Careers"

Sylvia's interest in cybersecurity was sparked when she was working as a system administrator and one of the workstations she managed was hacked. Since then, Sylvia has accumulated 20+ years of real-world experience in the field of cybersecurity. While focusing on firewalling, network security and data encryption, she is also eager to share her vast knowledge by training other cybersecurity professionals. Sylvia was the first woman to achieve the "Fortinet Network Security Expert Level 8" (NSE 8) certification and received the Fortinet Trainer of the year award for EMEA in 2022. Born and raised in Germany, Sylvia now lives and works in Switzerland where she loves to skydive in her free time. There too, she strives to share her knowledge as an instructor and coach and has participated in international competitions in 4-way formation skydiving as a member of the German female national team for three years.

**Optum Keynote: Barbara Kosloski**

Vice President of Technology, Optum at UnitedHealth Group

"Charting a Course in Times of Challenge"

Barbara Kosloski leads a team powering the technology in the people experience for the 350,000+ employees at UnitedHealth Group. She brings 28 years of experience in technology, transformation, and leadership, working previously at Target Corp., Slalom Consulting, and Accenture. She lives in Minneapolis, MN.

**Raytheon Keynote: Erin Heinmiller**

Executive Director, Global Infrastructure Services at Pratt & Whitney

"It is All About Risk, Both in Cybersecurity and Your Career"

Erin leads a team of skilled employees focused on developing the cloud, hosting, and network strategies to ensure company-wide availability. Her team is also responsible for improving the digital experience of over 42,000 employees worldwide through development of standards and deployment of collaboration capabilities.

With nearly 20 years of information technology experience, and a strong focus on cybersecurity, risk management and infrastructure, Erin led the development of secure, compliant, robust and scalable IT solutions before joining Pratt & Whitney while assuming positions of increasing responsibility at Raytheon Technologies and Sikorsky.

WiCyS
KEYNOTES

Enjoy the WiCyS 2023 Keynotes? Subscribe to the WiCyS Youtube channel to watch them post-conference.

Scan the code with your mobile phone camera to access.



THANK YOU TO OUR 2023 CONFERENCE SPONSORS

VIP SPONSORS

PREMIUM SPONSORS

DIAMOND SPONSORS

PLATINUM SPONSORS

GOLD SPONSORS

SILVER SPONSORS

CEU and CPE credits available by: CompTia, GIAC and (ISC)²

Make it happen here.

INTERNSHIP AND FULL-TIME ROLES

At Bloomberg, we use the power of technology to bring clarity to a complex world. In a career here, you'll help protect products that our global customers rely on to make critical financial decisions.



INTERNSHIP AND FULL-TIME ROLES

[Bloomberg.com/careers](https://www.bloomberg.com/careers)

Bloomberg

Make it
happen here.

THANK YOU TO OUR 2023 WiCyS COMMITTEES

CONFERENCE PROGRAM CHAIR

Ambareen Siraj

*NSF (Siraj is serving in her personal capacity)
Founder, WiCyS*

CONFERENCE GENERAL CHAIR

Janell Straach

*WiCyS Chair of the Board, Faculty,
Rice University*

PROGRAM CO-LEADS

Aisha Ali-Gombe

*Associate Professor,
Computer Science and Engineering,
Louisiana State University*

Jennifer Cheung

*Cybersecurity Research Scientist,
NIWC Pacific*

Ida Ngambeki

*Assistant Professor,
University of Maryland Baltimore
County*

Priyam Biswas

Offensive Security Researcher, Intel

Meg Layton

*Director of Information Security
Architecture and Engineering,
Children's National Hospital*

Elena Peterson

*Senior Cyber Security Researcher,
Pacific Northwest National Laboratory*

Chutima Boonthum

Professor, Hampton University

PROGRAM

Monika Akbar

*Assistant Professor,
The University of Texas at El Paso*

Rosie Hall

Security Research Engineer, Cisco

Karen Nemani

President, WiCyS Ontario Affiliate

Safwa Ameer

*Postdoctoral Researcher,
The Institute for Cyber Security at the
University of Texas at San Antonio*

Katherine Hutton

*Executive Director, UK/Europe
Partnerships, Cyber Capital Partners*

Jacqueline Ore

Cloud Security Analyst, Citi

Deborah Barnes

*Sr. Vulnerability and Threat Analyst,
Cradlepoint*

Arllyssa Jaquez

Network Security Architect, Verizon

Quintana Patterson

*IT Clinical and Compliance Manager,
University of Colorado Anschutz
Medical Campus*

Roshni Chandrashekhar

*Tech Lead Manager, OAuth Platform,
Google*

Amy Justice

*IT Security, Compliance and Privacy
Manager, Randstad NA*

Elizabeth Rasnick

*Assistant Professor,
Center for Cybersecurity at University
of West Florida*

Diara Dankert

Threat Researcher, ConnectWise

Chris Lemmon

*Advanced Security Engineer,
Secure Yeti*

Sarba Roy

Security Researcher, Intel Corporation

Mai Ensmann

*Assistant Cybersecurity Program
Manager, Cyber Florida*

Angel Liu

*Head of Governance, Risk and
Compliance, LinkedIn*

Jillian Seabrook

*Information System Security Manager,
MIT Lincoln Laboratory*

Maria Fanelle

*Networking and Security Engineer,
MITRE*

Dawn Mccarty-Jolly

Sr. Info Security Engineer, UHG/Optum

Amy Starzynski Coddens

*Strategic Partnerships Manager,
REN-ISAC/Indiana University*

Kathleen Gibson

*Penetration Tester,
Federal Reserve Bank of Richmond*

Aleise McGowan

*Treasurer,
WiCyS Neurodiversity Affiliate
Visiting Assistant Teaching Professor,
The University of Southern Mississippi*

Mike Zachman

VP and CSO, Zebra Technologies

Ashley Greeley

*National Cryptologic University, NSA
NCAE-C Program Team (K12 Lead)*

Sharon Mudd

*Sr. Cybersecurity Operations
Researcher,
Carnegie Mellon University Software
Engineering Institute*

Shafia Zubair

*Director, Supply Chain Cybersecurity
Risk Management, Johnson Controls*

THANK YOU TO OUR 2023 WiCyS COMMITTEES

SCHOLARSHIP

Janell Straach

Lead

WiCyS Chair of the Board
Faculty, Rice University

Gretchen Bliss

Director of Cybersecurity Programs,
University of Colorado Colorado
Springs

Jennifer Bush

Chief Information Security Officer,
Texas Department of Family and
Protective Services

Ramona Codreanu

Security Systems Administrator,
University of Michigan

Suzanne Dove

Solutions Architect Sr Staff,
Lockheed Martin

Marcie Friedman

Info Sec Technology Analyst,
Norfolk Southern

Esther Goldstein

Software Engineer, Data Security,
Salesforce

Anne Hall

Cyber Systems Security Engineer Sr
Staff, Lockheed Martin

Pushpa Kumar

Professor of Instruction,
University of Texas at Dallas

Alex Maestretti

CISO, Remitly

Danelle Mattison

Cyber System Security Engineer, Staff,
Lockheed Martin Skunk Works

Sharon Mireku

Executive Paralegal-Independent
Contractor, Law Firms-Both Private
and Corporate Environments

Lorie Pfannenstien

Program Director, Signals Intelligence
Collection Program (SICP) & Summer
Intern Program for Science and
Technology (SIPST), NSA

Penelope Rozhkova

Security Consultant, Accenture

Angela Sims-Ceja

Water Technical Operations
Superintendent, Aurora Water

Mary Wallingsford

Associate Professor,
Anne Arundel Community College

CAREER FAIR

Pat McCain

Lead

Globaux Source

Mary Jane Partain

Career Fair Concierge, Director,
UT Dallas

Tara Lewis

Career Coach,
Collin College (Frisco)

CAREER VILLAGE

Andrea Frost

Lead

Senior Software Security
Engineer, Dell Technologies

Stacie Bohanan

Principal Research
Scientist III, University of
Alabama in Huntsville

Terri Johnson-Akse

Instructor of Cybersecurity
Management,
UCCS College of Business

Mayra Paredes

SecOps Manager,
Southwire LLC

OPERATIONS AND LOGISTICS

Lynn Dohm

Lead

Executive Director, WiCyS

Peter Baldwin

vCFO, WiCyS

Tia DeBord

Registration Liaison, Globaux Source

Morgan Garland

Operations Manager, WiCyS

Colleen Huber

Marketing Coordinator, WiCyS

Kimberly Hutcherson

Meeting Space Coordinator,
Globaux Source

Pat McCain

Presenter Liaison, Globaux Source

Lana Richardson

Retail Store Management & Executive
Assistant to the Conference Chair,
WiCyS

Jessica Robinson

vCISO, WiCyS

Myrian Saint Jean

Financial Manager, WiCyS

Michele Tomasic

Director of Operations,
Carnegie Mellon University Software
Engineering Institute

Laura Villalobos

Community Manager, WiCyS

THANK YOU TO OUR 2023 WiCyS COMMITTEES

POSTER

Chutima Boonthum-Denecke

Lead

Professor/Director of IAC,
Hampton University

Idongesit Mkpong-Ruffin

Director,
Florida A&M University Center
for Cybersecurity (FCCS)

RETAIL STORE

Lana Richardson

Retail Store Management and Executive
Assistant to the Conference Chair,
WiCyS

Mia Partain

Retail Store,
WiCyS

Reethee Ghafoor

Retail Store,
WiCyS

SOCIAL MEDIA AND PR

Aditi Chaudhry

Cybersecurity Engineer,
Two Sigma

Midori Connolly

Customer Success Manager,
Yubico

Maddie Witt

Social Media Specialist,
WiCyS

Chelsea Conard

Consultant for Strategy, Risk, and
Compliance,
Kudelski Security

Alina Thai

Threat Intelligence Analyst,
Allstate

VOLUNTEER

Cameron Mitchell

Lead

Operations Coordinator,
Carnegie Mellon University Software
Engineering Institute

Jamie Glenn

Operations Coordinator,
Software Engineering Institute,
CERT

STRATEGIC PARTNERSHIP

YOUR BRAND ELEVATED

The future of women in the cybersecurity workforce lies in our hands. Champion the cause of recruiting, retaining and advancing women in cybersecurity by becoming a WiCyS Strategic Partner.

Your contributions are key to supporting WiCyS' year-round activities and helping women everywhere achieve their career goals in the cybersecurity field.

Scan the code with your mobile phone camera to learn more about strategic partnerships!



CYBER-SECURE YOUR FUTURE WITH FORTINET!!

Competitive Salary
Incentive Compensation
Stock Awards
Health Benefits
401K Matching
Career Growth
and More!

Fortinet makes possible a digital world that we can always trust through its mission to protect people, devices, and data everywhere. For nearly 20 years, we have built a culture of excellence. We are committed, hardworking and passionate about building the most successful cybersecurity company worldwide. We recognize our people and their contributions to fulfil this mission.

FORTINET

Search Opportunities:
www.fortinet.com/corporate/careers



PROGRAM PARTICIPATION TRACKS AND SESSIONS

- **TODAY'S TECHNOLOGY AND CHALLENGES TRACK**
Current issues and challenges, advances in research and development (R&D), and experimental findings.
- **LOOKING AHEAD TRACK**
Important technology/R&D trends, challenges on the horizon, upcoming solutions, and tomorrow's vision.
- **BEST PRACTICES TRACK**
Institutional/Operational/Academic best practices, tools, techniques, and approaches.
- **CAREER DEVELOPMENT TRACK**
Leadership and advancement.
- **GIAC, (ISC)², AND WICYS CPE TRACK**
Eligible for CPE credit from each organization.
- **COMPTIA CEU TRACK**
Eligible for A+, Network+, Security+, Linux+, Cloud+.

* Each colored dot represents a session track. Reference the colored dots throughout the agenda and session descriptions to identify each session's corresponding track(s).



TECHNICAL PRESENTATIONS

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



WORKSHOPS

Workshops are hands-on sessions (technical/professional development) on any topic related to cybersecurity. The audience is students, educators, professionals, and researchers (in any combination or by category). **Workshops are 2 hours long.**



BIRDS OF A FEATHER (BoaF)

Birds of a Feather are informal discussion sessions moderated by the facilitator 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.**



LIGHTNING TALKS

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



PANELS

Panels provide opportunities to discuss a current relevant topic in cybersecurity. In addition to the moderator, there can be up to 4 panelists. **Panels are 45 minutes long.**



STUDENT RESEARCH POSTERS

Student Research Posters provide opportunities for students to present their work for the audience at WiCyS in poster format. Winners in both undergrad and grad category receive travel support for a future security conference of their choice. Runners-up receive prizes as well.

2023 WiCyS SCHEDULE AT A GLANCE

THURSDAY		
7:00am - 7:00pm	Badge Pick-Up	Aurora Registration
9:30am - 11:30am	INVITE ONLY: Allyship Symposium and Breakfast	Cottonwood 6/7
11:00am - 6:30pm	WiCyS Store Open	Cottonwood 1
12:00pm - 1:30pm	INVITE ONLY: Senior Leader Luncheon	Juniper ABC
12:30pm - 1:30pm	First Timer's Panel	Adams B
12:30pm - 1:30pm	Recruiters Session	Adams C
12:30pm - 6:30pm	Capture the Flag (CTF) Mentoring	Spruce Foyer and Lobby
1:30pm - 4:30pm	Career Fair Setup by Sponsors	Aurora Exhibit Hall 1
2:00pm - 4:00pm	Workshop Series	Various Rooms
2:00pm - 6:30pm	Career Village Open	Adams A
2:00pm - 5:00pm	Career Village Talks	Cottonwood 2
4:00pm - 4:30pm	Break	
4:00pm - 7:00pm	Poster Session Check-In	Aurora Hall 1 Prefunction
4:30pm - 6:30pm	Workshop Series	Various Rooms
4:30pm - 5:25pm	Fireside Chat	Adams B
5:35pm - 6:30pm	Fireside Chat	Adams B
6:30pm - 7:00pm	Book Club Meetup	Charlton
6:30pm - 7:00pm	Community College Meetup	Adams C
7:00pm - 9:00pm	Socials	Juniper Ballrooms and Maple Meeting Rooms
7:00pm - 8:30pm	Educators/Scientists - Meetup with Funding Agencies	Summit 9
7:30pm - 9:00pm	Federal Scholarship Students Meetup and Networking Session	Summit 8

PICK-UP AND PURCHASE

WiCyS GEAR

Visit Cottonwood 1 for the WiCyS Store

THURSDAY 11:00am - 6:30pm

FRIDAY 9:45am - 6:00pm

SATURDAY 10:00am - 1:00pm

The WiCyS 2023 conference store will support the WiCyS conference scholarship fund. We thank you for your ongoing support and for wearing your WiCyS pride while paying it forward to more women in cybersecurity.

FRIDAY		
7:00am - 6:00pm	Badge Pick-Up	Aurora Registration
7:00am - 8:00am	Breakfast Available with Tables for Scholarship Recipients	Juniper A
7:00am - 8:15am	INVITE ONLY: Early Career Breakfast	Cottonwood 6/7
7:00am - 8:15am	INVITE ONLY: Mid Career Breakfast	Juniper B
7:00am - 8:30am	Poster Session Check-In	Aurora Hall 1 Prefunction
8:00am - 9:00am	Career Fair Setup by Sponsors	Aurora Exhibit Hall 1
8:30am - 9:45am	Conference Opening and Keynote (doors open at 8:15am)	Aurora Ballroom
9:45am - 11:45am	Career Fair Open	Aurora Exhibit Hall 1
9:45am - 11:45am	Capture the Flag (CTF) Mentoring	Spruce Foyer and Lobby
9:45am - 11:45am	Career Village Open	Adams A
9:45am - 11:45am	Career Village Talks	Cottonwood 2
9:45am - 11:00am	Student Poster Session and Networking Refreshment Break	Aurora Hall 1 Prefunction
11:00am - 11:45am	Presentation Sessions	Various Rooms
11:00am - 11:45am	Student Chapter Meetup	Adams D
12:00pm - 1:45pm	Lunch, Networking, and Keynote (must be seated by 12:10pm to eat)	Aurora Ballroom
1:55pm - 5:30pm	Career Fair Open	Aurora Exhibit Hall 1
1:55pm - 5:30pm	Capture the Flag (CTF) Mentoring Available	Spruce Foyer and Lobby
1:55pm - 5:30pm	Career Village Open	Adams A
1:55pm - 2:40pm	Presentation Sessions	Various Rooms
1:55pm - 2:40pm	Regional Affiliate Meetup	Adams D
2:40pm - 3:15pm	Break with Refreshments in Career Fair	Aurora Exhibit Hall 1
2:50pm - 4:40pm	Workshop Series	Various Rooms
4:45pm - 5:30pm	Birds of a Feather	Various Rooms
6:00pm - 7:45pm	Dinner, Networking, and Keynote (must be seated by 6:10pm to eat)	Aurora Ballroom
8:00pm - 9:00pm	Equity and Advancement Committee Meet and Greet	Summit 8/9
8:30pm - 11:59pm	Capture the Flag (CTF) After Dark Party	Spruce Foyer and Lobby

2023 WiCyS SCHEDULE AT A GLANCE

SATURDAY		
7:00am - 9:00am	Badge Pick-Up	Aurora Registration
7:00am - 8:15am	Military Breakfast	Juniper B
7:00am - 8:00am	Breakfast Available with Tables for Scholarship Recipients	Juniper A
7:00am - 5:00pm	Luggage Storage available (closed 9:30am to 10am)	Aurora Exhibit Hall 1
8:30am - 9:30am	Keynote (doors open at 8:15am)	Aurora Ballroom
9:30am - 10:00am	Group Picture and Break with refreshments	TBD
10:00am - 10:45am	Presentation Sessions	Various Rooms
10:00am - 10:45am	Lightning Talks	Adams D
11:00am - 11:45am	Presentation Sessions	Various Rooms
11:00am - 11:45am	Lightning Talks	Adams D
12:00pm - 12:45pm	Panels	Various Rooms
12:45pm - 2:00pm	Lunch, Closing Remarks and Awards (must be seated by 1:00pm to eat)	Aurora Ballroom
2:00pm - 2:30pm	Travel Stipend Verification	Aurora Prefunction
2:30pm - 4:30pm	Workshop Series	Various Rooms

TRACK COLOR KEY

- TODAY'S TECH AND CHALLENGES TRACK
- LOOKING AHEAD TRACK
- BEST PRACTICES TRACK
- CAREER DEVELOPMENT TRACK
- GIAC, (ISC)², AND WICYS CPE TRACK
- COMPTIA CEU TRACK (eligible for A+, Network+, Security+, Linux+, Cloud+)

CPEs & CEUs

GIAC, (ISC)² and WiCyS CPEs and CompTIA CEUs (eligible for A+, Network+, Security+, Linux+, Cloud+) are available for designated sessions. Reference the agenda or session descriptions and track key to identify the sessions that qualify.

After attending the full session, locate the WiCyS volunteer at the back of the room to scan the QR code or to have your badge scanned.

You must complete this step before leaving the session. There will be no credit given after the session is over.

You will receive an email by April which will include information on submitting to CompTIA, GIAC and (ISC)² to receive your CPEs/CEUs.

SOCIAL MEDIA






















CONNECT WITH THE WICYS COMMUNITY ON SOCIAL MEDIA!

Be a part of the collective strength of the WiCyS community! Follow us on Social Media!



2023 WiCyS SCHEDULE

THURSDAY AGENDA

TIME	DESCRIPTION	LOCATION
7:00am - 7:00pm	Badge Pick-Up	Aurora Registration
9:30am - 11:30am	INVITE ONLY: Allyship Symposium and Breakfast	Cottonwood 6/7
11:00am - 6:30pm	WiCyS Store Open	Cottonwood 1
12:00pm - 1:30pm	INVITE ONLY: Senior Leader Luncheon	Juniper ABC
12:30pm - 1:30pm	First Timer's Panel <i>Elizabeth K. Hawthorne, Esther Goldstein, Chyna Lane, Collins Okafor, Elizabeth Rasnick, Dianne Rose and Litany Hope Lineberry</i> 	Adams B
12:30pm - 1:30pm	Recruiters Session The Case for Neurodiversity in Cybersecurity: How Recruiters and Hiring Managers Can Attract, Develop, Grow and Retain Neurodivergent Talent <i>Kassandra Pierre and Aleise McGowan</i>   	Adams C
12:30pm - 6:30pm	Capture the Flag (CTF) Mentoring Available	Spruce Foyer and Lobby
1:30pm - 4:30pm	Career Fair Setup by Sponsors	Aurora Exhibit Hall 1
2:00pm - 4:00pm	Workshop Series (5 Concurrent)	
	Let's Get Logic(al): A Crash Course on Building Security Detections <i>Alexis Merritt and Holly Parrish Syed</i>   	Cottonwood 4/5
	Don't Let Your App Allow an Attack! Make Sure Your Open Source is Secure <i>Megan McIntyre and Diane Downie</i>    	Cottonwood 8/9
	CyberSleuths: Making Sense Out of Chaos Fusing CyberData and Intelligence Information <i>Elena Peterson and Ashley Billman</i>   	Adams B
	Integrated Risk Management with Tabletop Exercise <i>Lily Yeoh and Tauna Mills</i>   	Adams C
	Navigating Cybersecurity: Success and Retention <i>Cynthia Sutherland</i>    	Adams D
2:00pm - 5:00pm	Career Village Talks	Cottonwood 2
2:00pm - 6:30pm	Career Village Open	Adams A
4:00pm - 4:30pm	Break	
4:00pm - 7:00pm	Poster Session Check-In	Aurora Hall 1 Prefunction







CAREER VILLAGE

The WiCyS Career Village is a place for resume review, mock-interview guidance, career conversations, and professional headshots.

Located in Adams A
Thursday • 2:00pm - 6:30pm
Friday • 9:45am - 11:45am & 1:55pm - 5:30pm

2023 WiCyS SCHEDULE

THURSDAY AGENDA

TIME	DESCRIPTION	LOCATION
4:30pm - 6:30pm	Workshop Series (4 Concurrent)	
	AWS Security GameDay 2023 <i>Maya Flores and Danny Navo</i> 	Cottonwood 4/5
	Cybersecurity Career Exploration Via Virtual Reality <i>Michael Qaissaunee and Kyle Jones</i> 	Cottonwood 8/9
	Think Like an Adversary: Leveraging Artificial Intelligence to Optimize Tactics, Techniques and Procedures <i>Saskia Laura Schroeder</i> 	Adams C
	RIDE to Safety - Risk Assess the Next Conference <i>Meghan Jacquot, Samara Williams and Jessica Robinson</i> 	Adams D
4:30pm - 5:25pm	Fireside Chat Building a Robust Cybersecurity Ecosystem with Help From Federal Partners <i>Davina Pruitt-Mentle, Ashley Greeley and Albert Palacios</i> 	Adams B
5:35pm - 6:30pm	Fireside Chat Intel-Driven CyberDefense: How the IC Helps Drive Collective Defense <i>Morgan Adamski and Lauren Goldman</i> 	Adams B
6:30pm - 7:00pm	Book Club Meetup	Charlton
6:30pm - 7:00pm	Community College Meetup	Adams C
7:00pm - 9:00pm	Socials	Juniper Ballrooms and Maple Meeting Rooms
7:00pm - 8:30pm	Educators/Scientists - Meetup with Funding Agencies <i>Alice E. Smitley, Ashley Greeley and Jeremy J. Epstein</i>	Summit 9
7:30pm - 9:00pm	Federal Scholarship Students Meetup and Networking Session	Summit 8

CAREER VILLAGE TALKS

THURSDAY • Located in Cottonwood 2

- 2:00pm - 2:30pm • CybHER DivHERsity - Hacking the Glass Ceiling
- 2:30pm - 3:00pm • I Got Your Back: The Importance of Mentors and Sponsors
- 3:00pm - 3:30pm • The Career Path is a Road Trip
- 3:30pm - 4:00pm • Producing a Personal Brand
- 4:00pm - 4:30pm • The Marvelous Map of Cybersecurity Domains
- 4:30pm - 5:00pm • Navigating the Social Media Landscape

Changing health care for the better



Together, we can create a simpler, smarter,
more adaptive health care system

Our mission

To help people live healthier lives, and help make the health system work better for everyone.

About us

Optum®, part of the UnitedHealth Group® family of businesses, is a global organization that's evolving health care so everyone can have the opportunity to live their healthiest life. With our hands at work across all aspects of health, we connect people and information to create a healthier world, one insight, one connection and one person at a time.



Scan the QR code to apply
or visit **WorkAtOptum.com**

Follow us:

facebook.com/myOptum

linkedin.com/company/Optum

instagram.com/Optum






twitter.com/Optum

Optum

Diversity creates a healthier atmosphere: Optum is an Equal Opportunity/Affirmative Action employer and a drug-free workplace.
© 2023 Optum, Inc. All rights reserved.











2023 WiCyS SCHEDULE

FRIDAY AGENDA

TIME	DESCRIPTION	LOCATION
7:00am - 6:00pm	Badge Pick-Up	Aurora Registration
7:00am - 8:00am	Breakfast Available with Tables for Scholarship Recipients	Juniper A
7:00am - 8:15am	INVITE ONLY: Early Career Breakfast	Cottonwood 6/7
7:00am - 8:15am	INVITE ONLY: Mid Career Breakfast - Sponsored by Amazon and Verizon	Juniper B
7:00am - 8:30am	Poster Session Check-In	Aurora Hall 1 Prefunction
8:00am - 9:00am	Career Fair Setup by Sponsors	Aurora Exhibit Hall 1
8:30am - 9:45am	Conference Opening and Keynote (doors open at 8:15am) <i>*Coffee Available Before and During Keynote</i> Featured Speakers: <i>Kemba Walden, Office of the National Cyber Director; Blakely Wall, Verizon; Melissa Yandell, Walmart; Deborah Golden, Deloitte</i> Fortinet Keynote: Women in Cybersecurity: Creating Magic in Your Careers <i>Sylvia Schlaphof, Boll Engineering AG</i>	Aurora Ballroom
9:45am - 6:00pm	WiCyS Store Open (closed 12:00pm - 12:30pm for lunch)	Cottonwood 1
9:45am - 11:45am	Career Fair Open	Aurora Exhibit Hall 1
9:45am - 11:45am	Capture the Flag (CTF) Mentoring Available	Spruce Foyer and Lobby
9:45am - 11:45am	Career Village Open	Adams A
9:45am - 11:45am	Career Village Talks	Cottonwood 2
9:45am - 11:00am	Student Poster Session and Networking Refreshment Break	Aurora Hall 1 Prefunction
11:00am - 11:45am	Presentation Sessions (3 Concurrent) STRIDEing Through the Security Maze <i>Taylor Pyle and Jazmin Coronado</i>  Call for Input: Open Forum on National Cyber Workforce and Education Strategy <i>Suzanne Nielsen and Camille Stewart Gloster</i>  The Hacker Within, From IRC to Boardroom <i>Alyssa Miller</i>  Introduction to AI Red Teaming <i>Shiri Bendelac</i> 	Cottonwood 4/5 Cottonwood 8/9 Adams B Adams C
11:00am - 11:45am	Student Chapter Meetup: Grab a Seat in This Tribe of Fellow Students 	Adams D






2023 WiCyS SCHEDULE

FRIDAY AGENDA

TIME	DESCRIPTION	LOCATION
12:00pm - 1:45pm	Lunch, Networking, and Keynote (must be seated by 12:10pm to eat, Keynote starts at 12:30pm) Featured Speakers: <i>Archana Ramamoorthy, Google; Molly Moore, NSA; Korrey Anderson, SentinelOne</i> Optum Keynote: <i>Charting a Course in Times of Challenge</i> <i>Barbara Kosloski, Optum at UnitedHealth Group</i>	Aurora Ballroom
1:55pm - 5:30pm	Career Fair Open	Aurora Exhibit Hall 1
1:55pm - 5:30pm	Capture The Flag (CTF) Mentoring Available	Spruce Foyer and Lobby
1:55pm - 5:30pm	Career Village Open	Adams A
1:55pm - 2:40pm	Presentation Sessions (4 Concurrent)	
	Demystifying the Federal Resume and Application Process/How to Score a Dream Job in Public Service! <i>Amanda Martens</i> 	Cottonwood 4/5
	Stop the (OT) Apocalypse! Protecting the Nation's Critical Infrastructure <i>Radha Parikh</i> 	Cottonwood 8/9
	Next Big Attack in the CyberPhysical World: What to Expect and How to Protect Future Waves in CyberWarfare <i>Erin Joe</i> 	Adams B
	One Thousand Ways to Bypass MFA <i>Carly Battaile</i> 	Adams C
1:55pm - 2:40pm	Regional Affiliate Meetup: Grab a Seat in This Tribe of Peers 	Adams D
2:40pm - 3:15pm	Break with Refreshments in Career Fair	Aurora Exhibit Hall 1
2:50pm - 4:40pm	Workshop Series (5 Concurrent)	
	What's Special About Specialty Affiliates? 	Cottonwood 4/5
	Two Sides of a Coin: User Data Privacy, Security and Ethics of 5G Technology <i>Veena Ravishankar</i> 	Cottonwood 8/9
	Self Accountability and Challenging Our Own Bias <i>Jessica Robinson, Noreen Njoroge, Alyssa Miller, Jennifer Munoz, Quintana Patterson and Sofia Martinez</i> 	Adams B
	Adventure Guide to Cybersecurity Pro: How to Bring Your Existing Skillset into a Successful Future and Communicate Effectively <i>Courtney Hans</i> 	Adams C
	Workshop on National CyberWorkforce and Education Strategy <i>Suzanne Nielsen, Paul Tortora and Camille Stewart Gloster</i> 	Adams D

2023 WiCyS SCHEDULE

FRIDAY AGENDA

TIME	DESCRIPTION	LOCATION
4:45pm - 5:30pm	Birds of a Feather (5 Concurrent)	
	Security Research: Creating a Bridge Between Research Projects and Business Benefits <i>Jazmin Coronado and Glorianne Francavilla</i> 	Cottonwood 4/5
	Is the Juice Worth the Squeeze? Best Practices in Cybersecurity Vendor Management <i>Angie Kalaytowicz and Mary Diner</i> 	Cottonwood 8/9
	Artificial Intelligence and Race: Security or Surveillance? <i>Fatoumata Sankare</i> 	Adams B
	Navigating the Infosec World with Physical and Mental Illness <i>Elaine Harrison-Neukirch</i> 	Adams C
	Internships, Apprenticeships, Co-ops and Service Learning <i>Laura Malave</i> 	Adams D
6:00pm - 7:45pm	Dinner, Networking, and Keynote (must be seated by 6:10pm to eat, Keynote starts at 6:30pm) Featured Speakers: <i>Katie Boudreau, Mastercard; Pam Lindemoen, Cisco; Sharnikya Howard, Amazon</i> Raytheon Keynote: <i>It is All About Risk, Both in Cybersecurity and Your Career</i> <i>Erin Heinmiller, Raytheon</i>	Aurora Ballroom
8:00pm - 9:00pm	Equity and Advancement Committee Meet and Greet	Summit 8/9
8:30pm - 11:59pm	Capture the Flag (CTF) After Dark Party	Spruce Foyer and Lobby

CAREER VILLAGE TALKS

FRIDAY • Located in Cottonwood 2

- 9:45am - 10:15am • Hacking into Cybersecurity Careers
- 10:15am - 10:45am • CyberSecurity Leadership Sudoku
- 10:45am - 11:15am • Paradox of Career Advice: How to Build a Balanced Life
- 11:15am - 11:45am • Imposter Syndrome: Making It Without Faking It

Make your mark on a smarter, safer world

Staying ahead of evolving cyber threats requires solutions no one expects, especially adversaries. That's why we bring together diverse, unconventional thinkers to protect the world's most critical information.

Sound like you? Visit rtx.com/cybercareers








Raytheon
Technologies

COLLINS AEROSPACE | PRATT & WHITNEY | RAYTHEON INTELLIGENCE & SPACE | RAYTHEON MISSILES & DEFENSE






2023 WiCyS SCHEDULE

SATURDAY AGENDA

TIME	DESCRIPTION	LOCATION
7:00am - 9:00am	Badge Pick-Up	Aurora Registration
7:00am - 8:15am	Military Breakfast - Sponsored by Bloomberg, Lockheed Martin and Optum	Juniper B
7:00am - 8:00am	Breakfast Available with Tables for Scholarship Recipients	Juniper A
7:00am - 5:00pm	Luggage Storage available (closed 9:30am to 10am)	Aurora Exhibit Hall 1
8:30am - 9:30am	Keynote and Networking (doors open at 8:15am) <i>*Coffee Available Before and During Keynote</i> Featured Speakers: <i>Rebecca Moore, Shopify; Heather Vermillion, PACCAR; Aj'a Dehavalland Taylor, Palo Alto Networks</i> Keynote: <i>My WiCyS Stories</i> <i>Moderated by Aditi Chaudhry</i>	Aurora Ballroom
9:30am - 10:00am	Group Picture and Break with Refreshments	TBD
10:00am - 1:00pm	WiCyS Store Open	Cottonwood 1
10:00am - 10:45am	Presentation Sessions (4 Concurrent)	
	Mitigating Common Cognitive Biases in Cybersecurity Practice <i>Leigh Metcalf</i> 	Cottonwood 4/5
	Toto, I Have a Feeling We're Not in Web 2.0 Anymore: Security Considerations in Web 3.0 <i>Lisa Raykowski</i> 	Cottonwood 8/9
	PII: The Privacy Zombie <i>Alisha Kloc</i> 	Adams B
	Building a Talent Pipeline with Staff Internships <i>Allison Henry</i> 	Adams C
10:00am - 10:45am	Lightning Talks (all talks are in the same room) 	Adams D
	Not Lost in Translation: The Role of Non-Technical Leaders in Cybersecurity <i>Sasha Cohen O'Connell</i>	
	Great Student, Great Employee: How to Thrive During the Post-Grad Transition <i>Molly Soja</i>	
	User and Entity Behavior Analytics: The Future of Advanced Threat Detection <i>Apoorva Joshi</i>	
	How I Met My CybHER MentHER <i>Smruthi Sandhanam and Perri Nejib</i>	
	The Cybersecurity and Data Privacy Relationship <i>Angie Jin</i>	
	Making My Way Through Tech as a Neurodivergent, Queer, Woman of Color <i>Ruchira Pokhriyal</i>	
	Cyber-Informed Engineering and the Future of OT Security <i>Cheri Caddy</i>	
	Woody Woodpecker's Cybersecurity Lessons From 1957 <i>Camila Martins</i>	

2023 WiCyS SCHEDULE

SATURDAY AGENDA

TIME	DESCRIPTION	LOCATION
11:00am - 11:45am	Presentation Sessions (4 Concurrent)	
	Security Evaluation of Mental Health Care Applications and Web Services <i>Aishwarya Surani</i> 	Cottonwood 4/5
	Post-Quantum Cryptography: The Next Y2K or Security's Next Biggest Challenge? <i>Justin Simpson and Abby Willis</i> 	Cottonwood 8/9
	Just a Shift to the Left <i>Diane Stephens and Hanan Hibshi</i> 	Adams B
	PANEL: The Allyship Gap: Bridging the Gap Between the Actions Women of Color Find Meaningful and the Actions Others Prioritize <i>Kirsten Mitchell, Sunny Myers and Staci Hill Okine</i> 	Adams C
11:00am - 11:45am	Lightning Talks (all talks are in the same room) 	Adams D
	Real Talk: How to Navigate and Advocate as a Working Mom in Security Professions <i>Kavitha Sivagnanam</i>	
	We Are the 82% - The Value of Securing the Human Element Through Cybersecurity Awareness and Training <i>Julie Marquez</i>	
	Wait! They Said What? Hide Age and Years of Experience! <i>Deborah Kariuki</i>	
	The Skills I Needed to Succeed in Cybersecurity I Learned in Kindergarten <i>Debby Briggs</i>	
	It Takes a Village: A Case Study in Securing Electoral Landscapes <i>Jolie Grace Wareham</i>	
	Wandering the Wizarding World - Cybersecurity Concepts Through Harry Potter <i>Ann-Marie Horcher</i>	
	Full Speed Ahead: Accelerating the DoD's Dominance with Cloud Native Security <i>Caitlin Delmore</i>	
	Exploring Systems Thinking Through Gamification for Cybersecurity Training and Education <i>Olivia Schmidt and Alison Owens</i>	

MILITARY BREAKFAST

TOGETHER. WE SERVE.

The Military Breakfast will honor our veterans, those currently serving, military spouses, and those on active duty who are attending WiCyS 2023.

Sponsored by:









Bloomberg  **Optum**

Located in Juniper B
Saturday • 7:00am - 8:15am

*This event is by invitation only
and not open to all attendees!
RSVP is required.*

2023 WiCyS SCHEDULE

SATURDAY AGENDA

TIME	DESCRIPTION	LOCATION
12:00pm - 12:45pm	Panels (5 Concurrent)	
	Flying High: The Women of Aerospace Cybersecurity <i>Adrienne McCloud, Teresa Merklin, Erin Miller and Jenn Miosi</i> 	Cottonwood 4/5
	Hindsight: Reverse Engineering Successful Careers in Cybersecurity <i>Jummy Adejuyigbe, Tolu Onireti, Silka Gonzalez and Gatha Sadhir</i> 	Cottonwood 8/9
	Strategic and Tactical Views on the Evolution of Threat Intelligence <i>Harley Rohrbacher, Steph Shample, Kelsey Helms and April Lenhard</i> 	Adams B
	Politics, Partnerships and Incident Response <i>Cynthia Kaiser, Kozeta Garrett and Lauren McGlinch</i> 	Adams C
	CyberCrime Prevention and Investigation: A Case Study of Public, Private and University Partnership <i>Katie Shuck, Ashley Podhradsky, Arica Kulm and Kendra Russell</i> 	Adams D
12:45pm - 2:00pm	Lunch, Closing Remarks and Awards (must be seated by 1:00pm to eat) Featured Speakers: <i>Amy Tidwell, DeVry</i>	Aurora Ballroom
2:00pm - 2:30pm	Travel Stipend Verification	Aurora Prefunction
2:30pm - 4:30pm	Workshop Series (5 Concurrent)	
	CyberCareer Exploration (C2E) and Training for Transitioning Veterans and Military <i>Eric Brown and Vickie McLain</i> 	Cottonwood 4/5
	How Hard is Hardware Security? A Brief Journey to Learn the Fundamentals <i>Priyam Biswas</i> 	Cottonwood 8/9
	Attacking and Defending Public Cloud Environments <i>Dalal Alharthi</i> 	Adams B
	Forensics Workshop: Learn Foundational Crime-Solving Skills and How They Have Solved Cases of Injustices <i>Denise Dragos and Suzanna Schmeelk</i> 	Adams C
	Pivoting into Threat Intelligence - Using the KC7 Game to Learn Threat Intelligence Skills <i>Emily Hacker and Simeon Kakpovi</i> 	Adams D

WICYS CODE OF CONDUCT

We believe our community should be truly open for everyone. As such, we are committed to providing a safe and welcoming space for all. We invite all attendees, sponsors, speakers, and other participants to help us realize a safe and positive conference experience for everyone.

Scan the code with your mobile phone camera to view the full WiCyS Code of Conduct.



This is for you.

This conference. This career. This universe. Yes, for you.



Carnegie Mellon University
Software Engineering Institute

Secure the Future of Cybersecurity

Meet our staff at **Booth 206**
and join our effort in
solving the nation's
cybersecurity challenges.



Apply today!

Visit our website for more information.
sei.cmu.edu/go/wicys

2023 WiCyS CONFERENCE

PRE-CONFERENCE SESSIONS

TRACK COLOR KEY

- | | |
|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
|  TODAY'S TECH AND CHALLENGES TRACK |  CAREER DEVELOPMENT TRACK |
|  LOOKING AHEAD TRACK |  GIAC, (ISC) ² , AND WICYS CPE TRACK |
|  BEST PRACTICES TRACK |  COMPTIA CEU TRACK |

PRE-CONFERENCE SESSIONS

THURSDAY • 12:30PM - 1:30PM

First Timer's Panel

Room: Adams B

Track(s): 

Elizabeth K. Hawthorne, Esther Goldstein, Chyna Lane, Collins Okafor, Elizabeth Rasnick, Dianne Rose and Litany Hope Lineberry




Attending a WiCyS conference for the first time can be both exciting and daunting. There is just so much to navigate with so many choices in such a short time! For anyone experiencing the WiCyS conference for the first time, please join this session. Panelists from various backgrounds and interests will share their experiences of what they found useful, what mattered most and, most importantly, how to get the most out of this experience as a first-time WiCyS conference attendee.

PRE-CONFERENCE SESSIONS

THURSDAY • 12:30PM - 1:30PM

Recruiters Session | The Case for Neurodiversity in Cybersecurity: How Recruiters and Hiring Managers Can Attract, Develop, Grow and Retain Neurodivergent Talent

Room: Adams C

Track(s):   

Kassandra Pierre and Aleise McGowan

When neurodivergent candidates are funneled through poorly designed and executed talent pipeline programs, under the illusion of diversity, equity and inclusion, they are often subject to barriers and behavior that are personally and professionally injurious. The current model used to attract neurodiverse talent to roles in corporate America is broken. Companies tout their programs as being inclusive and supportive training grounds for stable careers. However, these programs are often well funded, well marketed and well...ineffective. After onboarding is complete, many neurodivergent candidates are met with the same exclusivity, permitted separatism and unapologetic ableism that prompted previous resignations. The Dandelion Model is used by companies to encourage new ways of thinking about neurodiversity. The challenge with the Dandelion Model is that the ingrained workplace culture that perpetuated stigma, enhanced stereotypes and resulted in employee separation is never challenged. How can leaders move past the Dandelion Model to create programs that attract, develop, grow and retain neurodivergent talent? In this talk, the presenter will outline actions organizational leaders can take to create and maintain talent programs and pipelines that support disabled and neurodivergent staff. These strategies are based on sound educational pedagogy and include the voices and expertise of disabled and neurodivergent workers while also being aligned to industry standards. They also allow for ongoing enrichment and training to match employee skill sets with key technical and non-technical roles. These strategies include guidelines that support equity, promote inclusion and ensure organizations compensate candidates for their talent regardless of ability.

WICYS PODCAST RELEASE



WiCyS is excited to announce the launching of a podcast in May 2023 to bring talented women together to celebrate and foster their passion and drive for cybersecurity.

We intend to deliver compelling stories, resources and experiences in a refreshing *"Wake up to WiCyS"* bi-weekly format.

2023 WiCyS CONFERENCE MEETUPS & CHATS

THURSDAY MEETUPS

Educators/Scientists - Meetup with Funding Agencies

Room: Summit 9 **Time:** 7:00pm - 8:30pm

Alice E. Smitley, Ashley Greeley and Jeremy J. Epstein

For educators and scientists, this session provides informal conversations with program directors/managers at various funding agencies such as NSF and NSA about potential funding opportunities related to cybersecurity.

Federal Scholarship Students Meetup and Networking Session

Room: Summit 8 **Time:** 7:00pm - 9:00pm

Come and meet fellow students participating in various federal scholarship programs. Learn about these programs and best practices by networking with peers/alums/federal employers.

FRIDAY MEETUPS

Student Chapter Meetup: Grab a Seat in This Tribe of Fellow Students

Room: Adams D **Time:** 11:00am - 11:45am

Track(s): ●

Join this session to learn about starting, running and maintaining a student chapter on campus. Current chapter leaders will share their experiences, discuss challenges and address the issues that commonly arise as a student chapter officer. This will be a freestyle session, so bring lots of questions with ideas and help each other succeed in promoting women in cybersecurity at their campuses.

Regional Affiliate Meetup: Grab a Seat in This Tribe of Peers

Room: Adams D **Time:** 1:55pm - 2:40pm

Track(s): ●

Come meet leadership from various affiliates as they form a freestyle discussion group to support all efforts by local affiliates. The group will discuss strategies, best practices, social media and more! Bring questions with ideas, and grow stronger together! They will talk about how to create/engage the local community. The discussion will be facilitated by WiCyS Ontario.

THURSDAY FIRESIDE CHATS

Building a Robust Cybersecurity Ecosystem with Help From Federal Partners

Room: Adams B **Time:** 4:30pm - 5:25pm

Track(s): ● ● **CPE Credits:** 1

Davina Pruitt-Mentle, Ashley Greeley and Albert Palacios

Federal efforts in the cybersecurity ecosystem are growing by leaps and bounds. Participants will have an opportunity to learn about existing and future federal initiatives underway to prepare, grow and sustain cybersecurity education and workforce development that safeguard and promote America's national security and economic prosperity. Representatives from the U.S. Department of Education, National Security Agency, Department of Defense, Department of Homeland Security, National Initiative for Cybersecurity Education within the Department of Commerce, and Department of Labor will provide an overview of program priorities, grant programs, workshops, webinars, conferences, apprenticeship and internship opportunities, professional development options, resources and other activities. Through an open and interactive conversation, participants will leave with a better understanding of the plethora of federal cybersecurity education and workforce development opportunities and how various government programs collaborate to build a whole-of-nation approach. The interactive forum will enable attendees to access resources and promote networking with agency representatives for collaboration. Speakers will encourage dialogue with the audience to learn how to improve federal efforts.

Intel-Driven CyberDefense: How the IC Helps Drive Collective Defense

Room: Adams B **Time:** 5:35pm - 6:30pm

Track(s): ● ● **CPE Credits:** 1

Morgan Adamski and Lauren Goldman

The Intelligence Community (IC) plays a significant role in providing context and warning to the cyberdefense community. Over the past few years, the way in which the IC collaborates with industry and academia has transformed into a fast-paced environment of integrating unclassified capabilities for analysis and information sharing while also maintaining a human-to-human component. This fireside chat will highlight challenges, success stories and best practices from operating an intel-driven model with the cybersecurity community.

2023 WiCyS CONFERENCE

WORKSHOP DESCRIPTIONS

WORKSHOP SERIES

THURSDAY • 2:00PM - 4:00PM

CyberSleuths: Making Sense Out of Chaos Fusing CyberData and Intelligence Information

Room: Adams B

Track(s):  CPE Credits: 2

Elena Peterson and Ashley Billman

Curious about the day in the life of a cybersecurity analyst? Like doing investigation, data analysis and solving puzzles? This interactive workshop will provide participants with the opportunity to act and think like a cybersecurity analyst by participating in a tabletop scenario where they will investigate a data breach incident, form hypotheses, test them against new information, and defend their conclusions about the most likely explanation about who stole the data and why. Cybersecurity analysis provides insight into the motivations, intent, tactics, techniques and procedures (TTPs) of cyberthreat actors focusing on the why and not just the how of cyberoperations. This insight allows organizations to prioritize their preemptive and mitigating actions to address vulnerabilities exploited by threat actors. It also supports decision makers in making informed, strategic-level decisions to support the confidentiality, integrity and availability of organizational assets. While the overall analysis workflow involves much more than the example this workshop will focus on, presenters will provide an environment that represents activities a cybersecurity analyst will face on a regular basis, providing a window into this career. Given the broad list of analysis elements, this session will focus on data fusion, investigative research, analytic rigor and report production. The session is split into one or more phases, where participants are provided specific sets of information that mimic the information a cybersecurity analyst would encounter, including any data analysis an analyst would perform. Additionally, tangential information that may not be part of the story may be provided. After each phase, participants will perform their investigative research, discuss in groups, and decide what they would advise their decision-makers based on the information available to them. Choices will be provided to which everyone provides their vote via a voting mechanism before individuals defend their choice. The distribution of votes from the participants will be displayed for all to see. No laptops will be required, as materials will be provided for this tabletop exercise. However, materials will be provided via Google Docs, and a phone or device will be needed to vote on choices. Participants with an interest in cybersecurity or analysis can use this session as a data point to determine their own career paths. Professionals in computing or related fields will have an opportunity to understand how cyberanalysis can benefit their own research and innovation goals. It is the hope that all participants will walk away with a positive and informed experience of the cybersecurity analyst profession.

Don't Let Your App Allow an Attack! Make Sure Your Open Source is Secure

Room: Cottonwood 8/9

Track(s):  CPE Credits: 2

Megan McIntyre and Diane Downie

Open Source Software (OSS) is hot! But with stories of exploits and stolen data, it can be scary! Creating secure software means making a code safe, but also knowing any security issues in OSS libraries. In this hands-on workshop, attendees will learn how to find vulnerabilities in the OSS they are using no matter the language or tech. As a result, participants will become fearless coding with OSS! Attendees will learn about software vulnerabilities and exploits using the 2017 Equifax breach and the 2021 Log4j Zero Day Vulnerability as examples. There will be a combination of presentation and hands-on exercises using free tools. Participants will review a sample code base to discover the OSS present, identify and remediate security risks. This workshop is designed for developers who have a basic understanding of programming but are new to using OSS or anyone else who wants to learn more about it. Attendees will be encouraged to work in small teams to foster a collaborative approach. Participants will get the most out of the workshop if they can use a laptop for the exercises, but this is not required. Hand-out sheets with the exercise steps will be provided to all attendees as well as a link to download the materials in a virtual setting. Attendees will leave this workshop with experience discovering OSS used in a project and the potential security issues associated with it as well as possible ways to remediate those issues. The workshop will provide information about where to go for additional learning.

Integrated Risk Management with Tabletop Exercise

Room: Adams C

Track(s):  CPE Credits: 2

Lily Yeoh and Tauna Mills

This workshop will introduce the concept of Integrated Risk Management (IRM) and explore the obstacles to and value of building an IRM program across an organization. Participants will ultimately be invited to discuss and decide whether or not IRM is a sustainable business practice and how to implement it in the workplace. The presenters will provide an overview of the key elements of an IRM program, including supporting technology, company culture, roles and responsibilities. The workshop will then break out into groups with tabletop moderators to answer several questions. Each group will assign a spokesperson and present their findings to the rest of the attendees before everyone discusses the overall findings. At the end, participants will be able to suggest steps they will take back to their companies/programs to build IRM programs inside their organizations.

2023 WiCyS CONFERENCE

WORKSHOP DESCRIPTIONS

Let's Get Logic(al): A Crash Course on Building Security Detections

Room: Cottonwood 4/5

Track(s):    **CPE Credits:** 2

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.

Navigating Cybersecurity: Success and Retention

Room: Adams D

Track(s):      **CPE Credits:** 2

Cynthia Sutherland

Cybersecurity means different things for people in different situations. Most look at it from the perspective of technology, cyberattacks, and as a demanding career with solid compensation. However, what is not discussed is what it takes to get in, stay in and be successful in the field, especially as a woman. Navigating a cybersecurity career can be even more of a challenge when a person has limited exposure, unconscious biases and are the only woman on the team. This workshop navigates attendees through the confidentiality, individuality and awareness pillars for a successful cybersecurity career, mental health as a security concern, and shows how representation does matter in cybersecurity. In this workshop, presenters will use cases for identifying and responding to the impact of cybersecurity on mental health

in high-performing and fast-paced environments. The goal of the workshop is to have participants walk away with tips on how to close the gaps in their performances, identify their uniqueness and value to an organization, and ideas on how to increase awareness of their capabilities in their organization. This workshop hopes to motivate women cybersecurity professionals to get in and stay in the field.

WORKSHOP SERIES

THURSDAY • 4:30PM - 6:30PM

AWS Security GameDay 2023

Room: Cottonwood 4/5

Track(s):    **CPE Credits:** 2

Maya Flores and Danny Navo

GameDay is a collaborative learning exercise that tests skills in implementing AWS solutions to solve real-world problems in a gamified, risk-free environment. This is a completely hands-on opportunity for WiCyS members to explore AWS services, architecture patterns, best practices and group cooperation. Like in all GameDay events, attendees will be placed in teams to support the fictitious startup, Unicorn, facing several vulnerabilities that will need to be secured in order for the business to operate. Secure Legends focuses on security incidents, such as ransomware attacks and other breaches, and will introduce participants to conducting forensics to prevent and remediate them. Attendees will be provided with a simulated environment containing common vulnerabilities they will secure using AWS services like IAM, Network Firewall, Backup, Systems Manager and more. All attendees and different experience levels are welcome to participate! WiCyS players will be broken up into teams of four and given a starting architecture they will need to evolve throughout the day in response to internal and external events. There is no one right answer; the path that GameDay participants take is up to them, based on the AWS resources at their disposal in pre-packaged AWS accounts.

2023 WiCyS CONFERENCE

WORKSHOP DESCRIPTIONS

Cybersecurity Career Exploration Via Virtual Reality

Room: Cottonwood 8/9


Track(s):    **CPE Credits:** 2

Michael Qaissaune and Kyle Jones

Presenters will provide an overview of an NSA-funded project to build a virtual reality experience for students to explore cybersecurity careers. In addition to describing the genesis and goals of the project, they will detail plans for the future of the environment and the possibility of applying them across other cybersecurity domains and extending the functionality. The RING cybersecurity career orientation 3D virtual experience establishes the foundation for teacher, student and parent awareness and understanding of cybersecurity careers and opportunities. Existing career awareness instructional resources lack structure, interaction and engagement and fail to enable students to visualize themselves in what seems like mysterious workplaces. Over the last five years, there has been significant growth in 3D virtual worlds for e-learning and distance education. These immersive environments create complex, highly interactive simulations using in-world work environments and interactive exercises. Virtual learning environments enable students to practice skills and master the application of concepts and abilities in a work-based educational context. These environments offer the ability to manage content presentation, integrate challenges and implement meaningful student competency assessments. The presenters built and populated a 3D virtual reality career exploration experience that allows students to explore an environment with seven virtual reality rooms, avatars, artifacts and Easter eggs to learn about different careers within the seven NIST NICE Workforce Framework Cybersecurity categories. After a brief demonstration of the environment, a walkthrough of the controls and an overview of the scenario/mission, participants will get an opportunity to immerse themselves in virtual reality and explore the environment independently.

RIDE to Safety - Risk Assess the Next Conference

Room: Adams D

Track(s):    **CPE Credits:** 2

Meghan Jacquot, Samara Williams and Jessica Robinson

To get here today, people made hundreds if not thousands of decisions, many based on risk assessment. Today's workshop will direct attendees on how to threat model a conference, and do risk assessment and open source intelligence information gathering. The leaders of this workshop have a mission to share the tools they need to stay safe. This workshop spans multiple domains of cybersecurity with a focus on personal and physical safety. Attendees can expect to walk through aspects of preparing to attend a conference with a focus on securing their data, privacy, location, and have a general awareness of threats that likely occur during

conferences from registration through attendance. As part of this workshop, attendees also will get experience building their skills around open source intelligence and threat modeling/risk assessment during several hands-on activities. Then there will be a debrief to discuss findings and how to apply these simple concepts to cybersecurity as a whole. Participants will leave with skills and perspectives to continue this practice at other conferences and apply it to their lives. Together, the group will RIDE to safety with risk awareness, investigations, decisions and examinations.

Think Like an Adversary: Leveraging Artificial Intelligence to Optimize Tactics, Techniques and Procedures

Room: Adams C

Track(s):     **CPE Credits:** 2

Saskia Laura Schroeder

Artificial intelligence (AI) can offer a huge strategic and tactical advantage for organizations in the context of cybersecurity. There is a general agreement that AI can help organizations better defend and protect their critical infrastructure, employees, reputation and more. But could AI be exploited by attackers for their purposes? What does this mean for defenders? Given the growing amount of publicly available data and openly accessible AI toolkits, chances are high that attackers are, or will be, leveraging AI to drive attacks that are more targeted, more sophisticated, more automated and executed on a larger scale. In this interactive workshop, participants will learn about AI applications, specifically Natural Language Processing and Computer Vision, in the field of offensive security. Presenters will introduce the structure of the cybersecurity Kill Chain and proceed with a hands-on exercise focusing on real-world attacks. Participants do not need any specific prior knowledge to participate. The session will review a set of machine-learning algorithms, which could be applied to automate and optimize one or more attack steps. Participants will have the opportunity to work in small groups. Then, participants will review the attack steps and analyze which parts could be enhanced with AI. Finally, the group will share the results across all attack stages and discuss the risks and likelihood of adversaries adopting AI in the future.

2023 WiCyS CONFERENCE

WORKSHOP DESCRIPTIONS

WORKSHOP SERIES

FRIDAY • 2:50PM - 4:40PM

What's Special About Specialty Affiliates?

Room: Cottonwood 4/5

Track(s): ●

CPE Credits: 2

The WiCyS Affiliate program doesn't just include those based in specific geographic locations, they also have specialty affiliates that represent certain subfields in cybersecurity, specific communities of people and special interest topics. The beauty of the specialty affiliates is they bring together a community of global WiCyS members who are tied together by a distinct commonality so that they can work together to explore how to use that common thread to support the WiCyS mission. Hear updates from the leaders of some of these specialty affiliates about their goals for the year and some of the discussions and topics that drive their respective affiliates. The programs represented will include WiCyS Colors of Inclusion; WiCyS Latina; WiCyS Cloud Security; WiCyS BISO; WiCyS Privacy, Law and Policy; and WiCyS Pride.

Two Sides of a Coin: User Data Privacy, Security and Ethics of 5G Technology

Room: Cottonwood 8/9

Track(s): ● ● ● ●

CPE Credits: 2

Veena Ravishankar

Mobile technologies are rapidly evolving to provide faster and better services, for example 5G being rolled out. 5G has advanced characteristics to support user needs to provide higher data rates, ultra-low latency, massive connectivity, seamless mobility, reliability and high availability, flexibility and programmability, energy, cost and spectrum efficiency. With advancements in technology and their ubiquity, the security threats evolve, bringing along a plethora of challenges as well as responsibility of securing user data. This workshop addresses the two sides of user data privacy within 5G technology: How to achieve it in 5G via new techniques and tools, and the privacy and ethical concerns it brings. Participants will explore algorithms and tools that help achieve privacy in 5G networks through hands-on exercises. Then, participants will consider related ethical issues through a guided discussion of a case study involving privacy. Participants will leave with an enhanced knowledge of some technical aspects of 5G and the ethical issues surrounding this new generation of networking. Students, educators and everyone else interested in this topic is welcome to attend and will be provided access to necessary software during this workshop.

Self Accountability and Challenging Our Own Bias

Room: Adams B

Track(s): ● ● ● ●

CPE Credits: 2

Jessica Robinson, Noreen Njoroge, Alyssa Miller, Jennifer Munoz, Quintana Patterso and Sofia Martinez

The WiCyS Equity Advocacy Committee (EAC) will present a workshop on the internal biases everyone has and strategies for growth and change. This includes self-accountability, taking responsibility for how people show and respond to others who are different or where people have certain preconceived notions about age, ethnicity, race, gender, where someone is from, how one speaks or dresses and more. This workshop will explore the definition of implicit bias and other biases (unconscious, confirmation, etc). It will allow participants to actively engage in activities and discussions where they can become more aware of their own bias. This will include a self-test on implicit bias as well as a short video to help in grounding the discussion. The EAC also will share the work they have been doing on behalf of WiCyS to support gender equity within the organization, and it looks forward to hearing from attendees on what is most important as a member of WiCyS regarding this topic.

MEMBERSHIP BENEFITS

AMPLIFY YOUR NETWORK. AMPLIFY YOUR PORTFOLIO. AMPLIFY YOUR CAREER.

Enjoy year-round benefits of engagement with a unique and powerful community of peers in academia, research, industry and government. Share ideas, best practices, experiences and more with thousands of women in cybersecurity!






Scan the code with your mobile phone camera to check out all the benefits!

2023 WiCyS CONFERENCE

WORKSHOP DESCRIPTIONS

Adventure Guide to Cybersecurity Pro: How to Bring Your Existing Skillset into a Successful Future and Communicate Effectively

Room: Adams C

Track(s):   

CPE Credits: 2

Courtney Hans

It's no secret that innovation is a direct benefit of diverse perspectives and experience; so ask what in an individual's past can they bring to play for the future? This workshop is meant for both new and seasoned security professionals as it is focused on how to leverage a diverse skill set during a job search, as well as how to use communication skills effectively in a security role. Presenters will discuss how to connect the message to what's relevant to a company's unique audience, engender idea co-creation and buy-in, and compel the audience to action, whether that audience is a new employee going through security training or an executive whose approval is needed to resource someone else's work. In her third major career transition, this speaker brings two wildly different decades of experience into a new decade of focus on cybersecurity. Before pursuing an MBA and career in experiential product strategy, this workshop host was an adventure travel guide for a worldwide active travel company, leading type-A travelers (many of whom were executives at their own companies) around the globe. Adventure travel guiding, just like security work, requires a cool head during a crisis, the ability to make a plan and then dozens (if not hundreds) of new ones to balance proactive and reactive work, and the ability to maintain a reserve of energy for when things really hit the fan. Using leadership trips and tricks (along with a few funny guide and travel stories), extensive audience participation, partner feedback, and role-based scenarios, this workshop will engage participants in a conversation on how to hone both informal and formal leadership skills in discussions and coalition building around security strategy and risk management. Come prepared to dissect resumes and/or LinkedIn with a new friend, practice interview skills, and role-play interactions with C-suite executives, board members and new employees.

Workshop on National CyberWorkforce and Education Strategy

Room: Adams D

Track(s):     

CPE Credits: 2

Suzanne Nielsen, Paul Tortora and Camille Stewart Gloster

The Office of the National Cyber Director has been working with partners in the Executive Office of the President and interagency, as well as experts from academia, nonprofits, the private sector and civil society, to produce a National Cyber Workforce and Education Strategy. The strategy addresses four main issues: federal cyber workforce, national cyber workforce, cyber education and training, and digital awareness. The purpose of this workshop will be to draw on the WiCyS community, including professionals, students

and educators, to obtain feedback on the strategy's key pillars, strategic objectives and next steps, including plans to implement the initiatives called for in the strategy. This session complements another technical presentation that will share the content of the strategy, whereas this workshop will provide an open forum for obtaining feedback and additional ideas about strategy implementation and any other issues still to be addressed.

WORKSHOP SERIES

SATURDAY • 2:30PM - 4:30PM

CyberCareer Exploration (C2E) and Training for Transitioning Veterans and Military

Room: Cottonwood 4/5

Track(s):    




CPE Credits: 2

Eric Brown and Vickie McLain

This workshop will introduce the C2E program at Tennessee Tech and the training environment developed on the CEROC Cyber Range. Participants also will be given an opportunity to complete exercises within the environment with assistance from the environment developers.

How Hard is Hardware Security? A Brief Journey to Learn the Fundamentals

Room: Cottonwood 8/9

Track(s):   

CPE Credits: 2

Priyam Biswas

Hardware security is increasingly becoming vital in ensuring the security assurance of the product pipeline. With hardware security issues on the rise, research has shown that around 63% of organizations have encountered security breaches due to hardware vulnerabilities in 2019. As the complexity of the hardware designs are growing rapidly, hardware security issues can range from access control and hardware backdoor to side channels and IP piracy. Unlike software vulnerabilities, patching or resolving any post production hardware vulnerability is extremely difficult, expensive and sometimes infeasible. Therefore, it is important to have a good understanding of hardware security to combat these attack scenarios. In this workshop, attendees will embark on a journey to understand the basic concepts of hardware security, threat modeling in hardware security, different attack scenarios and state-of-the-art best practices in mitigating hardware security issues. The workshop is suitable for all stakeholders in the field of cybersecurity, starting from the students and young professionals who want to take their first step in hardware security domain up to leaders and experts who are working on resolving hardware vulnerabilities. This workshop is designed as a mix of lectures




2023 WiCyS CONFERENCE

WORKSHOP SESSIONS

and group activities to offer attendees a deep understanding of hardware security issues. Participants will need to bring their own laptops but are not required to install any additional software or hardware. A VM will be provided before and during the workshop.

Attacking and Defending Public Cloud Environments

Room: Adams B

Track(s):   




CPE Credits: 2

Dalal Alharthi

Many organizations are moving to the cloud at a rapid pace due to benefits such as cost-effectiveness, scalability, reliability and flexibility. This increases the need for security professionals to protect critical commercial and government cloud infrastructure from cyberattacks. Unfortunately, demand currently far exceeds the supply of highly qualified cloud security professionals. This workshop aims to contribute to resolving this issue by going through different cloud security roles to build the capacity critically important to national security. To secure cloud environments, the Cloud Shared Responsibility Model is used to address that cloud providers are responsible for its security while the customers are responsible for the security in the cloud. This workshop aims to shed some light on how to secure what is in the cloud and is designed to go through different cloud security roles from the perspectives of the red team (attackers), the blue team (defenders) and the yellow team (developers). This is an intermediate-level workshop designed to cover 40 to 50% of content of the AWS Cloud Practitioner Certificate. Bring a laptop to create a free AWS and Splunk account.

Forensics Workshop: Learn Foundational Crime-Solving Skills and How They Have Solved Cases of Injustices

Room: Adams C

Track(s):   

CPE Credits: 2




Denise Dragos and Suzanna Schmeelk

This workshop showcases skills needed for foundational digital forensics (DFR) fieldwork and explains pedagogical techniques and successful environments for building inclusive classrooms that have been successful as reported by heterogeneous students. Forensics topics demoed and discussed will be selected from the following areas found in a foundational digital forensics course: data acquisition; processing crime/incident scenes; information retrieval from Windows, Macintosh and Linux systems; recovering graphic, Word, Acrobat and other file types; virtual machine forensics; investigating emails; examining social media data; writing investigation reports; studying the importance of ethics for expert witnesses; and understanding expert testimony in digital investigations. The skills learned from this workshop will overview a full semester course, which covers the basics

for cybercrime and cyberincidents to prepare students for interaction with law enforcement agencies, organizational forensic teams and digital forensic courses. This workshop will highlight cases that the presenters have worked on throughout their careers and provide demos on a simulated crime scene case. They will discuss the DFR process and procedure for investigating digital evidence recently recovered from a simulated crime scene. The workshop will guide the audience through the process and encourage them to participate in their own investigation with the use of tools demoed. Attendees will be encouraged to participate along with the lead investigator presenters as they walk through needed foundational skills in digital forensics.

Pivoting into Threat Intelligence - Using the KC7 Game to Learn Threat Intelligence Skills

Room: Adams D

Track(s):   

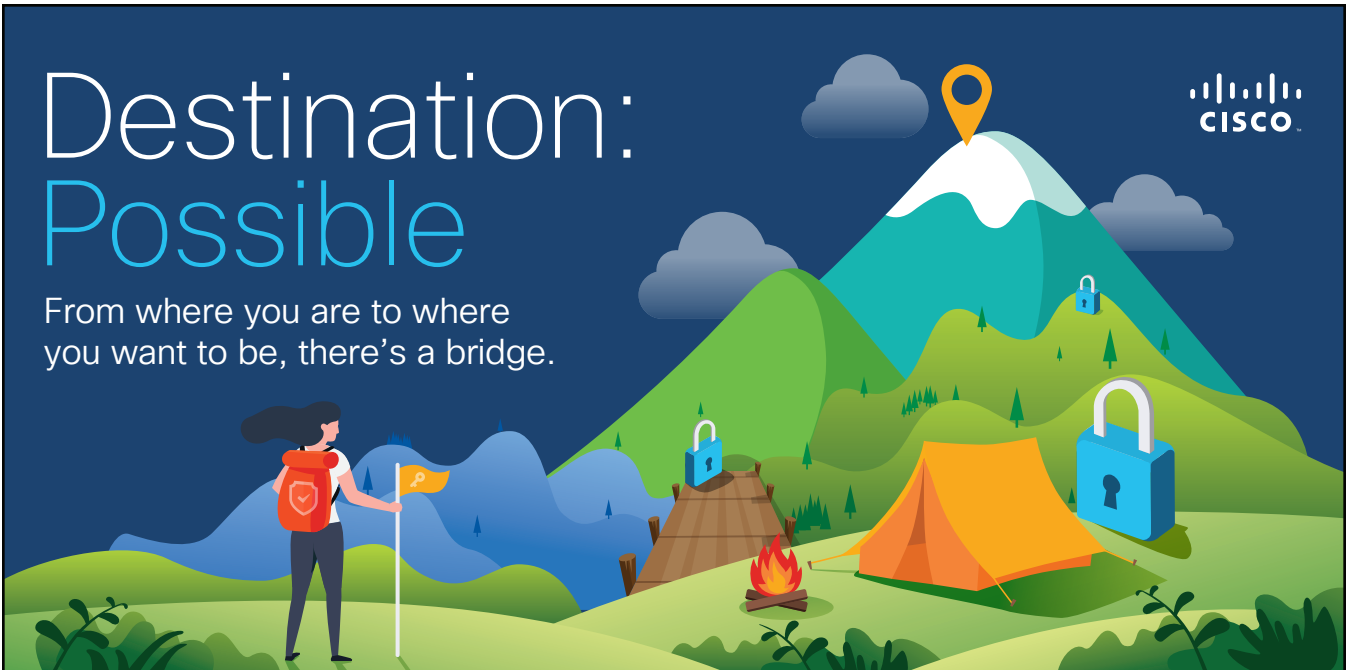
CPE Credits: 2

Emily Hacker and Simeon Kakpovi

One of the primary skills needed for threat intelligence is the ability to pivot through a dataset and find malicious activity. But how can people who hope to get into threat intelligence possibly learn these skills without already having a job that grants them access to these types of datasets? Historically, this has been challenging, so the presenters are thrilled to introduce KC7, a game designed to teach individuals the skills necessary for threat intelligence by utilizing a simulated dataset. In this workshop, attendees will: Learn how to use Kusto Query Language (KQL) to manipulate data in Azure Data Explorer clusters, Pivot across simulated datasets, including email, web browsing, passive DNS, and endpoint data to learn how TI analysts identify adversary techniques, tools and infrastructure, and Implement protections and mitigations to disrupt threat actor activity. During this workshop, attendees will learn the tools and techniques used by threat intelligence analysts to identify the most sophisticated threat actors. They'll then apply these techniques to identify malicious activity within logs stored in Azure Data Explorer clusters. Attendees will learn how to group threat actor signals, implement protections and mitigations, and better understand how to protect customers from these advanced threats.

Destination: Possible

From where you are to where
you want to be, there's a bridge.



Discover what's possible: cisco.com/go/bridgethegap

Learn more: trust.cisco.com

© 2023 Cisco and/or its affiliates. All rights reserved.

Deloitte.

Want to do what's next now?

Join Deloitte Cyber & Strategic Risk

Learn more at
deloitte.com/us/cyberjobs



Copyright © 2023 Deloitte Development LLC. All rights reserved.

2023 WiCyS CONFERENCE

PRESENTATION SESSIONS

TRACK COLOR KEY

- | | |
|-------------------------------------|--------------------------------------------------|
| ● TODAY'S TECH AND CHALLENGES TRACK | ● CAREER DEVELOPMENT TRACK |
| ● LOOKING AHEAD TRACK | ● GIAC, (ISC) ² , AND WICYS CPE TRACK |
| ● BEST PRACTICES TRACK | ● COMPTIA CEU TRACK |

PRESENTATION SERIES

FRIDAY • 11:00AM - 11:45AM

STRIDEing Through the Security Maze

Room: Cottonwood 4/5

Track(s): ● ● CPE Credits: 0.75

Taylor Pyle and Jazmin Coronado

With the accelerating rates of cybersecurity incidents and new vulnerabilities, securing and monitoring assets for malicious behaviors has become increasingly important. However, it can be difficult to do so without having a good understanding of what should be protected and how those assets can be compromised. With many different security options and paths available, not knowing where to start or even which direction to look can feel similar to being stuck in a maze. Automated security tools have their benefits, but often leave an incomplete picture due to the lack of contextual product details and network connection concerns. This is where threat modeling and abuse cases come in. Threat modeling allows individuals to understand their threat landscape and how the assets can be compromised or exploited from a holistic view. Abuse cases are constructed off the application's behavior, which details how the current implementation can be abused and manipulated to an attacker's benefit. These processes are collaborative, informative and, most importantly, human driven. A major benefit to introducing these processes is that they can be easily customized based on customer needs and resources. Modeling allows for greater insight into how different components interact at every layer and gives a complete picture of the system. A popular framework for threat modeling is STRIDE - spoofing, tampering, repudiation, information disclosure, denial of service and escalation of privileges. STRIDE aids in categorizing and representing diverse tactics an adversary or insider threat may take to compromise an asset. Once the threat model process is completed, the results can be used to help prioritize and discover what to monitor, detect, mitigate and understand how future vulnerabilities may affect the asset. This presentation will introduce what threat modeling is and help guide the audience on how to conduct a threat model using the STRIDE framework and abuse cases, along with lessons learned to make the process more efficient.

Call for Input: Open Forum on National Cyber Workforce and Education Strategy

Room: Cottonwood 8/9

Track(s): ● ● CPE Credits: 0.75

Suzanne Nielsen and Camille Stewart Gloster

The Office of the National Cyber Director has been working with partners in the Executive Office of the President and interagency, as well as experts from academia, nonprofits, the private sector and civil society, to produce a National Cyber Workforce and Education Strategy. The strategy addresses four main issues: federal cyber workforce, national cyber workforce, cyber education and training, and digital awareness. This presentation will explain the motivation for the creation of a strategy to address these issues as well as the process used to gather the ideas that inform its content. The bulk of the presentation will be devoted to laying out the strategy's key pillars, strategic objectives and next steps, including plans to implement the initiatives called for in the strategy.

Introduction to AI Red Teaming

Room: Adams C

Track(s): ● ● CPE Credits: 0.75

Shiri Bendelac

As artificial intelligent (AI) systems become ubiquitous in day-to-day life, it is vital to evaluate and understand their weaknesses and vulnerabilities. These inherent risks exist across data collection, data processing, storage and deployment. AI red teams simulate adversaries in order to erode the ability of AI systems to accomplish their goals. This can be mitigated by building off cybersecurity best practices, detection methods and defenses against these attacks. Different adversarial threat models pose different levels of threat depending on the level of access to the attacked system. In the white box threat model, an adversary acquires complete access to a trained model's weights. In the black box threat model, the adversary is only able to perform queries to the model. Both attacks can have dire consequences such as lowering the efficacy of a system or leaking sensitive information. In this talk, AI security engineers from The MITRE Corporation will share lessons learned in this burgeoning field and showcase industry tools such as ATLAS, a threat modeling tool for AI systems. This will provide a primer on AI red teaming, emphasize the impact on high-stake scenarios and raise awareness about this rapidly growing field.

2023 WiCyS CONFERENCE

PRESENTATION SESSIONS

The Hacker Within, From IRC to Boardroom

Room: Adams B

Track(s): ● ●

CPE Credits: 0.75

Alyssa Miller

Here's the unlikely story of how a bullied 12-year-old got a job, bought a computer, hacked into one of the most prominent online communities of the time, and three decades later stands at the pinnacle of her career in cybersecurity as the CISO of a global organization. Forged in the IRC chatrooms of 90s hacker culture, she stumbled and triumphed through a series of serendipitous twists and turns to build a successful career, going from a misfit hacker to a cybersecurity executive. In this session, the presenter will share the story of how she navigated a journey from that 12-year-old with a passion for technology through her various roles in technology and security and is now in the C-Suite. Attendees will learn from the many twists and turns and lessons learned along her path. She will describe how she's used her own origin story to hack the minds of directors in some of the toughest boardrooms on Wall Street. She'll show you how embracing authenticity created extreme acceleration in achieving her career aspirations and discuss where these lessons can be applied throughout anyone's career journey. She'll also share the key to successfully entering the community, thriving in growth and achieving heights never thought possible. Attendees will leave this session with knowledge of how to overcome common obstacles, leverage opportunity effectively, and impact the digital world with all the vigor of a 12-year-old hacker.

review resumes and provide tips and tricks they learned over decades in the federal sector. This session will help job seekers search through job postings on USAJobs.gov and prepare professional resumes reflecting skills, knowledge and education that are relevant to the job they are pursuing. Topics include: How to read a vacancy announcement on USAJobs.gov, How to know which announcements are the best to apply for, Learn what is specialized experience and why it matters, and Learn some resume writing techniques that will help pass the first cut in the federal application process. Candidates should see higher resume referral rates when applying to federal positions, which means the job seeker's resume is sent to a hiring manager for consideration, and hopefully increases the job seeker's chances of being invited to interview for a position.

Stop the (OT) Apocalypse! Protecting the Nation's Critical Infrastructure

Room: Cottonwood 8/9

Track(s): ● ● ●

CPE Credits: 0.75

Radha Parikh

In February 2021, a hacker was able to change the chemical levels at a Florida water treatment plant to dangerous levels. The attack was contained because an employee happened to notice the cursor on the screen moving automatically. Shortly after, a ransomware attack on one of the largest pipeline companies disrupted gasoline deliveries on the east coast, leading President Biden to pass an executive order recognizing cyberthreats to the nation's critical infrastructure. The order emphasized the need for controls to protect operational technologies (OT) in the wake of geopolitical tension and national security. This presentation will further dive into real world cyberattacks on critical infrastructure and introduce how securing OT comes into play. Participants from various cyberroles can learn essential OT terms, architectures, and current trends at a high level to build a common language. Through a demonstration, they will learn how MITRE ICS framework and SIEM solutions can be implemented to maintain the core tenets of safety, reliability and availability of OT devices.

PRESENTATION SERIES

FRIDAY • 1:55PM - 2:40PM

Demystifying the Federal Resume and Application Process/How to Score a Dream Job in Public Service!

Room: Cottonwood 4/5

Track(s): ● ● ●

CPE Credits: 0.75

Amanda Martens

Ever wonder what it takes to realize the dream of working in public service? Look no further! The Cybersecurity and Infrastructure Security Agency's Talent Management team is here to demystify the federal resume as well as the federal application process and help make dreams a reality! Learn from some of the agency's top recruiters on how resumes differ when applying to federal positions, how to showcase relevant experience, and what hiring managers are looking for during resume reviews. Presenters also will overview the federal application process, break through federal jargon on job announcements and what to expect after applying. Recruiters will be on hand to answer questions,

The Next Big Attack in the CyberPhysical World: What to Expect and How to Protect Future Waves in CyberWarfare

Room: Adams B

Track(s): ● ●

CPE Credits: 0.75

Erin Joe

Everyone needs to know about the next big cyberattack and ways to prepare for it. This presentation provides inside details from the front line examination of nation state attacks such as those from Russia against Ukraine and the energy sector as well as from China against those engaged in activities threatening their plan for dominance. It brings

2023 WiCyS CONFERENCE

PRESENTATION SESSIONS

in firsthand knowledge of the Colonial Pipeline attack to share leader-level considerations for businesses hit by ransomware revealing the range of decisions needed based on their knowledge, confidence and business practices. It also illustrates all the types of government activity that occurs in response to attacks against critical infrastructure and prepares businesses to engage not only in the investigative response but also in the legal and policy processes that follow a significant cyberincident. Nation states are using information campaigns to promote false information across many media forms. This presentation shows some of the more active IO campaigns to help the audience understand the breadth of their targeting. Given these actual examples, it is likely the next big attack will involve a complex combination of cyber and IO attacks along with the potential for physical attacks or threats. This presentation provides the vision not only of future attacks but also of the tactical and strategic ways leaders can best prepare proactively to maximize readiness and response.

One Thousand Ways to Bypass MFA

Room: Adams C

Track(s): ● ●

CPE Credits: 0.75

Carly Battaile

It's 9 a.m. on Monday morning, and someone gets a call from a friend asking why they emailed her a weird link for an important document she can't open. The email must have been compromised, but how is that possible? This person has a strong password and multi-factor authentication (MFA) on the account, so there's no way a threat actor could've gotten in...right? It was only a matter of time. Threat actors have found plenty of ways to bypass MFA and get into users' accounts. For years, security professionals have been urging individuals and businesses to enable MFA for their accounts. Now that it's become an industry standard, threat actors are finding new ways to get around those second or third factors. Whether through social engineering, a technically sophisticated phishing site or simply by annoying the user until they relent, it is becoming easier for threat actors to access accounts. This presentation will cover some of these attack patterns that threat actors employ to get around MFA challenges on accounts they are targeting. In particular, presenters will go into detail on how reverse proxy phishing sites work and how incident responders can spot this activity in their logs. Diving into the technical side, they also will discuss the research and testing of a sample phishing kit - Evilginx2 - as an example of how effective these attacks can be. As the group discusses ways MFA can be circumvented, participants will leave this talk understanding why it is so important to have multiple layers of security beyond MFA. Many of these attacks can be mitigated by the use of hardware MFA or FIDO2 tokens, so the group will finally discuss this method of authentication and why it is much harder to bypass.

PRESENTATION SERIES

SATURDAY • 10:00AM - 10:45AM

Mitigating Common Cognitive Biases in Cybersecurity Practice

Room: Cottonwood 4/5

Track(s): ● ●

CPE Credits: 0.75

Leigh Metcalf

Humans are the central characters in the use and defense of technology. They bring powerful capabilities to solve cybersecurity problems, but brains aren't perfect. Cybersecurity presents a huge volume of information to process simply to keep up. Cybersecurity professionals, therefore, rely on mental shortcuts to process this onslaught of information, identify anomalies and fix problems. However, not all these heuristics are appropriate. Some are skewed by cognitive biases and others by fundamental misunderstandings. There are over 150 known biases in psychology, and this talk will describe five of the most common that negatively influence cybersecurity. There also will be tips on how to reduce the hazards and produce better responses to the information you must process to not only keep up but also thrive in the process. The session will conclude with recommendations for identifying, diagnosing and mitigating biases in general. There are no magic cures, but awareness can help people slow down and think carefully when the stakes are high.

Toto, I Have a Feeling We're Not in Web 2.0 Anymore: Security Considerations in Web 3.0

Room: Cottonwood 8/9

Track(s): ● ●

CPE Credits: 0.75

Lisa Raykowski



As more companies bring their brands to the Metaverse and many people interact with Web 3.0 technologies, security strategy needs to be considered. There is a much greater awareness around security today than back when Web 2.0 was emerging. Whether an early adopter or a skeptic, Web 3.0 is here, and people are in the metaverse gaming, using cryptocurrencies or being impacted by AI and machine learning. Web 3.0 technologies must demonstrate to companies and users that they are protected and safe. This session will take participants through the evolution of Web 3.0 and its current state. The presenter will go under the hood of Web 3.0 and provide an overview of the core idea of its architecture (e.g., decentralization). There will be examples of reliable Web 3.0 technologies in use today and top security concerns (e.g., anonymity) takeaways. Attendees will walk away with actionable defenses to explore while embracing Web 3.0 technologies.

2023 WiCyS CONFERENCE

PRESENTATION SESSIONS

PII: The Privacy Zombie

Room: Adams B

Track(s):  



CPE Credits: 0.75

Alisha Kloc

The concept of PII, or personally identifying information, has guided critical decisions around privacy for years. Companies, governments and consumers believe that protecting a specific, limited subset of data points, such as name or social security number, is sufficient to protect an individual's privacy. But they're dangerously wrong. Like a horror movie zombie, the term PII reached the end of its useful life a long time ago yet continues to lurch around chewing on the brains of engineers and policymakers alike. This presentation will begin by examining how companies dutifully lock away data labeled PII then collect and use all other data without limitation. As one privacy scholar noted, the current information economy is the most highly surveilled environment in the history of humanity. Companies build enormous dossiers about consumers then claim such data is anonymous because PII is not linked to the millions of data points about each consumer. Next, presenters will debunk misconceptions about what information is personally identifying. The only way to guarantee protection of consumers' personal data – to not collect it – isn't acceptable for most companies. Many kinds of data have genuinely valuable uses beyond advertising or selling. Presenters will cover the best ways to protect consumer data that don't rely on the outdated concept of PII and share suggestions for how to implement these in practice. The talk will close with a call for the entire tech industry to radically rethink how to collect, use and protect the data harvested from consumers. Every company that collects consumer data must consider that any piece of information could potentially identify the person it belongs to and treat all data accordingly. It's time to slay the PII zombie for good.

Building a Talent Pipeline with Staff Internships

Room: Adams C

Track(s):  

CPE Credits: 0.75

Allison Henry

Addressing the challenges of the information security workforce shortage with the budget of a public higher education institution requires creative thinking, especially in the hyper-competitive San Francisco Bay Area tech market. With multiple retirements and vacant positions left unfilled, the UC Berkeley Information Security Office looked into strategies for building an internal talent pipeline rather than relying on external recruitments to fill senior positions on the team. To support this strategy, in 2019 the university launched the Staff Internship Program, where staff working in IT roles in other departments work part-time with the information security team for a fixed period of time. This program benefits: Participants by building skills and providing professional development opportunities, Departments by building cybersecurity skills that improve their IT services,



The Information Security Office with additional FTE for project and operational work, and The campus by increasing the number of IT staff with cybersecurity knowledge and experience. In this presentation, a presenter will share her own experience entering the information security workforce through an informal staff internship opportunity and how it inspired a desire to formalize the program and increase access outside of informal networks. The team will discuss lessons learned on building a successful program, including documenting MOUs, selecting appropriate work assignments, training and development, and integrating part-time interns into the team culture. The team also will share testimonials from program participants and how they benefited with time for Q&A.

PRESENTATION SERIES

SATURDAY • 11:00AM - 11:45AM

Just a Shift to the Left

Room: Adams B

Track(s):  

CPE Credits: 0.75

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.

2023 WiCyS CONFERENCE

PRESENTATION SESSIONS

Post-Quantum Cryptography: The Next Y2K or Security's Next Biggest Challenge?

Room: Cottonwood 8/9

Track(s):  



CPE Credits: 0.75

Justin Simpson and Abby Willis

The crypto landscape is rapidly changing. Many of the encryption systems used today are based on binary algebraic methods. These methods are easy to solve in one direction, but impossible to solve in the other unless someone holds the secret key. A new super computer is being developed that will completely change the ability to secure data in the traditional way. Quantum computers are based on quantum mechanics, which allows it to perform computer operations at an exponentially more efficient rate than a regular computer. Once a quantum computer is fully realized, all existing asymmetric and digital signatures and key exchanges will immediately become ineffective. The presenters will walk the group through cryptography today and steps that can be taken today to begin preparing any company, network and individual for a world where post quantum computers could be readily available and used.

Security Evaluation of Mental Health Care Applications and Web Services

Room: Cottonwood 4/5

Track(s):  



CPE Credits: 0.75

Aishwarya Surani

Several sectors in everyday life have adopted digitization, especially health care, which accelerated further due to the COVID-19 pandemic. People use telehealth services in the form of web services and mobile applications. These services include regular health checkups, scheduling appointments, and sometimes providing mental health care support to patients. Given the nature of these services, especially when dealing with mental health, users share sensitive and personal information online through websites or mobile applications for consultation. Such technological arrangements bring additional risk to users privacy and security. To evaluate this further, a full-scale security evaluation of 48 web services and 40 mobile applications in the mental health care domain was conducted. Results show that mental health care web services follow expert security standards and protocols, such as SSL certification, robust authentication schema and others. On the other hand, mobile applications need to analyze further significant security factors such as permissions, encryption algorithms and certificates as people use these applications more frequently. This session will provide actionable recommendations that are imperative to follow for all applications and web services due to the sensitivity of data shared in these services.

PANEL: The Allyship Gap: Bridging the Gap Between the Actions Women of Color Find Meaningful and the Actions Others Prioritize

Room: Adams C

Track(s):  

CPE Credits: 0.75

Kirsten Mitchell, Sunny Myers and Staci Hill Okine

This talk will discuss what true allyship and advocacy look like, what actions individuals can choose to create change, how people can adjust their behaviors, and how to listen to understand not just respond. From personal experiences and extensive data sets, presenters will share examples of what folks do (or don't do), what actions are seen as having the most value, varying risks, and how to think beyond just intent to actual impact. The most recent McKinsey Women in the Workplace Reports (2021 and 2022) inspired this conversation, stating, "There's a notable disconnect between the allyship actions women of color say are most meaningful and the actions white employees prioritize. Although white employees recognize that speaking out against discrimination is critical, they are less likely to recognize the importance of more proactive, sustained steps such as advocating for new opportunities for women of color and stepping up as mentors and sponsors. This talk leans heavily on both research and candid and vulnerable personal experiences. With experience in tech, the presenters have found this is highly relevant to the experiences of many underrepresented people based on gender or race.



Learn about our Women+Tech Scholars Program™

DeVry.edu

©2023 DeVry Educational Development Corp. All rights reserved.



Adrienne A.
Current Women+Tech Scholar



More power, less emissions.

Renewables and natural gas will help drive towards a cleaner energy future. Help to build a more sustainable world, a world that works for all of us.



Power your career with purpose. [gecareers.com](https://www.gecareers.com)



2023 WiCyS CONFERENCE

BIRDS OF A FEATHER

TRACK COLOR KEY


- | | |
|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
|  TODAY'S TECH AND CHALLENGES TRACK |  CAREER DEVELOPMENT TRACK |
|  LOOKING AHEAD TRACK |  GIAC, (ISC) ² , AND WICYS CPE TRACK |
|  BEST PRACTICES TRACK |  COMPTIA CEU TRACK |

BIRDS OF A FEATHER

FRIDAY • 4:45PM - 5:30PM

Security Research: Creating a Bridge Between Research Projects and Business Benefits

Room: Cottonwood 4/5

Track(s):   CPE Credits: 0.75

Jazmin Coronado and Glorianne Francavilla

Research can be an exciting endeavor, especially in the ever-changing and expansive world of cybersecurity. Due to the variety of specialties in this field, focusing on one subject area can be difficult. The speakers will share their experience being on a dynamic team, where they have the autonomy to dictate a research engagement if it ties back to a potential risk reduction and security posture improvement for the business. They will share insights on how to convey research objectives and convince the business side of an organization of the positive impacts, along with the different types of research activities one could engage in and its potential benefits. The speakers will reflect on their experience engaging in various research activities, starting book clubs, and ensuring activities stay related to business needs. Research topics and examples that may be covered in this presentation include, but are not limited to, cloud infrastructure, Internet of Things, red teaming activities, exploit development, certifications, boot camps and honeypots.

Is the Juice Worth the Squeeze? Best Practices in Cybersecurity Vendor Management

Room: Cottonwood 8/9

Track(s):   CPE Credits: 0.75

Angie Kalaytowicz and Mary Diner

In an industry with thousands of vendors for cybersecurity solutions, how do businesses know if they're making the right choice? For a given solution, how do they know which is the right cybersecurity vendor to choose? Should they build their own cybersecurity solution instead? What happens when a vendor is acquired? How do they know if they're getting the value expected out of a vendor? How do they navigate the renewal process? Who should they partner with? During this Birds of a Feather session, presenters will share best practices for navigating cybersecurity vendor management and open the discussion for others to share their experiences in cybersecurity vendor management.

Artificial Intelligence and Race: Security or Surveillance?

Room: Adams B

Track(s):    CPE Credits: 0.75

Fatoumata Sankare

Today, with the advancement of technology, investigative searches are not only physical but also digital. With electronic devices such as cellphones and computers no longer being considered a luxury device but an essential device, law enforcement is now relying on evidence extracted from these items in criminal investigations. Digital devices contain massive amounts of data that can be useful in not only criminal matters but national security-related instances as well. The problem is that the data on these devices contain information that may be deemed private to citizens. Law enforcement has been using the Fourth Amendment to justify their use of digital evidence. However, the Fourth Amendment does not explicitly factor in digital evidence. The policies are not up to date with the procedures used by law enforcement, and citizens may be paying for it through the invasion of privacy. With the increased use of artificial intelligence, the biggest question becomes is it security or surveillance, and which communities are negatively impacted or targeted?

2023 WiCyS CONFERENCE

BIRDS OF A FEATHER

Navigating the Infosec World with Physical and Mental Illness

Room: Adams C

Track(s): ● ●

CPE Credits: 0.75

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.

Internships, Apprenticeships, Co-ops and Service Learning

Room: Adams D

Track(s): ● ● ●

CPE Credits: 0.75

Laura Malave

Students and career changers can use internships, apprenticeships, co-ops and service learning to gain experience in cybersecurity. In this session, presenters will discuss the different forms of experiential learning and benefits and disadvantages of each. This presentation also will include tips and tricks for searching for and securing entry-level cybersecurity positions. In addition, the benefits to employers of implementing experiential learning programs will be discussed. Participants will be encouraged to share their experiences searching for internships and entry-level cybersecurity positions as well as their perspective from within those positions. Employers also will be encouraged to share how applicants can stand out from the crowd for success when searching for internships and entry-level cybersecurity positions.

CAPTURE THE FLAG (CTF) COMPETITION

OFFERED BY: NATIONAL CYBER LEAGUE (NCL)

The WiCyS 2023 Capture the Flag (CTF) competition will be offered at the 2023 conference by WiCyS strategic partner National Cyber League (NCL). All conference registrants (students and non-students) were invited to register and compete in this virtual event, taking on realistic industry skill-based challenges designed to test and build participants' hands-on cybersecurity skills. The CTF is a great way for attendees to challenge themselves, compete with other cyber enthusiasts and learn something new along the way.



The CTF kicks off on **Thursday, March 16 at 12:30pm** and ends on **Friday, March 17 at midnight**. CTF coaching is available in the Spruce Foyer and Lobby, so participants can get help with challenges and meet other CTF players as well as the NCL team. To wrap up the event, there also will be a CTF After Dark Party with plenty of swag, snacks and fun shenanigans for all participants.

Winners will be announced during the closing remarks and awards ceremony on March 18. There will be leaderboards for students and non-students with prizes awarded to top players.

Registration for the CTF took place prior the conference.

CTF Mentoring

Spruce Foyer and Lobby

Thursday • 12:30pm - 6:30pm

Friday • 9:45am - 11:45am and 1:55pm - 5:30pm

CTF After Dark Party

Spruce Foyer and Lobby

Friday • 8:30pm - Midnight



Every day you're **safer** with Google

We keep more people safe online than anyone else in the world with products that are **secure by default**, **private by design** and **put users in control**.



If you are passionate about building systems that protect users and working at massive scale on a stunning array of technologies and challenges, then we'd love to meet you.

Find current opportunities with Security and Privacy teams
g.co/SecurityPrivacyEngJobs

 Security Engineering

LEVEL UP



Investigate. Analyze. Develop. Operate. Protect.

The latest video games are no match for an exciting career in cybersecurity.

Join a company where anything is possible. We have the bandwidth.

Do you?

mastercard.com



Mastercard is a registered trademark, and the circles design is a trademark, of Mastercard International Incorporated. © 2021 Mastercard. All rights reserved.

2023 WiCyS CONFERENCE

PANEL SESSIONS

TRACK COLOR KEY

- | | |
|-------------------------------------|--------------------------------------------------|
| ● TODAY'S TECH AND CHALLENGES TRACK | ● CAREER DEVELOPMENT TRACK |
| ● LOOKING AHEAD TRACK | ● GIAC, (ISC) ² , AND WICYS CPE TRACK |
| ● BEST PRACTICES TRACK | ● COMPTIA CEU TRACK |

PANEL SESSIONS

SATURDAY • 12:00PM - 12:45PM

Flying High: The Women of Aerospace Cybersecurity

Room: Cottonwood 4/5

Track(s): ● ● **CPE Credits: 0.75**

Adrienne McCloud, Teresa Merklin, Erin Miller and Jenn Miosi

Aerospace is a dynamic industry open to students and current practitioners. It is a borderless world that's part of a country's critical infrastructure. Aerospace encompasses airports, airlines, outer space, spacecrafts and satellites. As a result, the industry faces business and national security challenges. According to the European Air Traffic Management Computer Emergency Response Team report for 2020, attacks on civil aviation increased by 530%. In October 2022, Russian-speaking hackers took responsibility for an attack that brought down websites for 14 airports. This panel consists of women on the frontlines securing the aerospace industry. Job growth is on the rise in the aerospace industry. The U.S. Bureau of Labor Statistics expects jobs to grow by 6% between 2021 and 2031. In early 2022, "The Guardian" reported that the United Kingdom reported a 39% increase in the aerospace industry within the last five years. Now is the best time to move into an aerospace career. This presentation has four parts. The audience will first learn about the aerospace environment. Next, panelists will introduce and discuss their professional backgrounds, challenges and successes as well as provide tips for being successful in the aerospace industry. In part three, the panel will give their viewpoints on a relevant topic. Finally, there will be a question and answer period. Audience members will interact with panelists, revisit previous comments or bring up any additional industry topic not covered. Presenters also will provide links for learning more about the aerospace industry. Key takeaways are links for career opportunities, tips for getting noticed in the application process, and an understanding of the complexity of the aerospace sector.

Hindsight: Reverse Engineering Successful Careers in Cybersecurity

Room: Cottonwood 8/9

Track(s): ● ● **CPE Credits: 0.75**

Jummy Adejuyigbe, Tolu Onireti, Silka Gonzalez and Gatha Sadhir

It's only with hindsight that people can look back and pinpoint the pivotal moments and decisions that helped shape their careers. A new skill learned, a challenge accepted or even a career-altering failure can all add up to success. The problem with hindsight is that it only comes after one of those defining moments has passed. What if individuals could better recognize these moments and decisions in real time? If they could better understand what these pivotal moments were for someone else, how they handled them or what they wish they did differently, individuals could reverse engineer their success and apply it to their own development. To help WiCyS attendees do just that, five remarkable women have come together who are at the forefront of their respective industries to share their successes, failures and guidance on developing a career in cybersecurity. Moderated by a leader in vulnerability management, the panel will discuss questions from the moderator to help arm attendees with insights they can use to recognize key moments in their own careers and achieve success in the cybersecurity field. This panel consists of leaders in vulnerability management, cloud security, maritime cybersecurity, regulatory governance and compliance from investment banking, technology, consulting and travel industries.

2023 WiCyS CONFERENCE

PANEL SESSIONS

Strategic and Tactical Views on the Evolution of Threat Intelligence

Room: Adams B

Track(s): ● ●

CPE Credits: 0.75

Harley Rohrbacher, Steph Shample, Kelsey Helms and April Lenhard

Threat actors have existed for decades. Understanding their motives, mission, target attack behaviors and more is critical to mitigating their actions. This panel will explore the evolution of threat intelligence and how each company approaches it. The discussion also will review different types of threat intelligence, such as: Strategic- high-level info on changing risk and the threat landscape (executive level, long-term use, bigger picture), Operational- details of specific campaigns, such as how it was carried out and the motive (defenders, high-level, short-term use), Tactical- attacker TTPs (security architects, low-level, long-term use to track attackers), and Technical- indicators of specific tools like malware (SOC staff & IR, low-level and short-term use as indicators can constantly change). The panel also will discuss best practices for leveraging cyber threat intelligence, the threat intelligence life cycle, threat data vs. threat intel vs. threat hunting, and some key challenges in using threat intelligence. Attendees will gain insight into threat intelligence advancement and approaches and take away lessons learned and best practices across industries to apply at their places of work.

CyberCrime Prevention and Investigation: A Case Study of Public, Private and University Partnership

Room: Adams D

Track(s): ● ●

CPE Credits: 0.75

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.

Politics, Partnerships and Incident Response

Room: Adams C

Track(s): ● ●

CPE Credits: 0.75

Cynthia Kaiser, Kozeta Garrett and Lauren McGlinch

On July 15, 2022, Iran attacked Albanian government networks causing critical public service outages across the nation while fueling insecurity and chaos throughout the country. What came soon after was one of the most unprecedented government responses to a cyberincident: the Albanian prime minister severed diplomatic ties with Iran and ordered all diplomatic staff to leave. This action was facilitated in large part by rapid U.S. government and private sector incident response and support to the Albanian government. The deployed teams worked side-by-side and with the Albanian government to restore digital services, attribute the attack to Iran, investigate intrusion vectors and adversary activity across the networks, and share identified indicators of compromise with network defenders across the world. All the while, Iran continued to threaten, leak data, and conduct activity against government networks. At the same time, the teams briefed senior Albanian officials about the progress, results and impact of the attacks. These technical and intelligence support teams directly supported political decision making in Albania and with allies across the globe. On this panel, conference participants will hear from the director of one of the primary Albanian government agencies involved, the lead of the private sector incident response and recovery team, and the lead U.S. government cyberanalyst deployed in the country as they discuss the technology challenges and political dynamics they faced, the close partnership with each other and the Albanian government, and the career experiences that prepared them for this event. The panel will be moderated by a U.S. government executive who worked with U.S. policymakers and the deployed teams to translate the incident response efforts into U.S. policy decisions. Conference participants will hear four women discuss how they leveraged their years of experience countering cyberthreats to support political decisions on the world stage.



NSA CYBERSECURITY WE'RE HIRING!

At NSA, have the best of both worlds: A meaningful career and work-life balance.

We offer competitive salary and benefits and unmatched purpose: At NSA, you can protect our democracy, privacy, security, and way of life from our adversaries.

You can also travel the world, receive tuition assistance, and enjoy an abundance of leave options, including vacation time, sick leave, paid parental leave, paid time off for physical fitness, and more...

www.intelligencecareers.gov/nsa



U.S. Citizenship is required. NSA is
an Equal Opportunity Employer.



PACCAR

is proud to be participating in WiCyS 2023 - come see us!

Named one of the
"Top Companies for Women to Work
For in Transportation"
in 2022 by the
Women in Trucking Association.



 **KENWORTH**

 **Peterbilt**

 **DAF**

PACCAR is a global technology leader in the design, manufacture and customer support of high quality light-, medium- and heavy-duty trucks under the Kenworth, Peterbilt and DAF nameplates. PACCAR also designs and manufactures advanced powertrains, provides financial services and information technology, and distributes truck parts related to its principal business.

2023 WiCyS CONFERENCE

LIGHTNING TALKS

TRACK COLOR KEY

- | | |
|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
|  TODAY'S TECH AND CHALLENGES TRACK |  CAREER DEVELOPMENT TRACK |
|  LOOKING AHEAD TRACK |  GIAC, (ISC) ² , AND WICYS CPE TRACK |
|  BEST PRACTICES TRACK |  COMPTIA CEU TRACK |

LIGHTNING TALKS

SATURDAY • 10:00AM - 10:45AM

All Talks are in Room: Adams D

Track(s):      **CPE Credits: 0.75**

Not Lost in Translation: The Role of Non-Technical Leaders in Cybersecurity

Sasha Cohen O'Connell

Being the FBI's chief policy advisor for science and technology without a technical background seems like a terrible idea. However, while serving in that senior executive role, the presenter learned that despite a non-technical background, their acumen in facilitating decision-making, translating technical issues for lay audiences, and building cross-sector teams were exactly the skills required. Through this lightning talk, the presenter will make the case that the cyber workforce is missing out on needed key talent by narrowly focusing on those with technical inclinations and overemphasizing technical curriculum. To solve this gap, participants will be challenged to build upon their experiences and lessons learned at American University School of Public Affairs, where they created the first-of-its-kind undergraduate and graduate cyber curriculum taking a non-technical approach to ensuring that all students are considering their potential role as future leaders in cybersecurity and cyber and tech policy.

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.

User and Entity Behavior Analytics: The Future of Advanced Threat Detection

Apoorva Joshi

With the threat landscape evolving constantly and attacks becoming more complex, writing rules to catch all possible attack scenarios is becoming increasingly impractical. This is especially true in the case of advanced attacks, such as insider threats, which touch multiple credentials, IP addresses, and machines to move laterally within an organization. Another challenge with rules is they lack context and may miss incidents that are never seen before, such as zero-day attacks. This is where User and Entity Behavior Analytics (UEBA) can help. In this presentation, they will talk about a new category of security solutions that uses machine learning techniques to model the standard behavior of entities in a corporate environment, detect abnormal behavior, and determine if this behavior has security implications. Topics include: components of a UEBA solution, UEBA use cases in Security, Advantages of UEBA over traditional security tools, and a case study of how UEBA can help detect advanced threats.

How I Met My CybHER MentHER

Smruthi Sandhanam and Perri Nejib

In this session, a cyber software engineer and her mentor, a senior fellow working in cybersecurity, will discuss how a fateful meeting at a panel discussion at an engineering conference led to a mentorship opportunity that changed both of their lives. The speakers will take attendees on the journey they went through from 2018 until now as mentor and protege, how that relationship has transpired over time, and the impact it has had on both of their careers and personal lives. Each speaker will reflect on their experiences and discuss the importance of networking at conferences and establishing a diverse, collaborative environment as part of an overall professional toolkit. In addition, the positive impact of mentorship for both mentor and mentee will be examined by this successful relationship.

2023 WiCyS CONFERENCE

LIGHTNING TALKS

The Cybersecurity and Data Privacy Relationship

Angie Jin

In 2018, the General Data Protection Regulation (GDPR) went into effect. It was, and still is today, considered one of the most extensive legal frameworks for the protection of personal data. GDPR has set the standard and become the baseline for a wave of new privacy legislation sweeping the globe. After GDPR came the California Consumer Privacy Act (CCPA) and later the California Privacy Rights Act (CPRA). Today, about 137 out of 194 countries have put in place legislation for data protection and privacy. The increase of data privacy laws comes with great protection for personal data and great responsibility for complying with these regulations, which impacts many departments in organizations, such as IT, HR, InfoSec, etc. Data protection laws require organizations to keep personal data safe through security. Privacy and cybersecurity are interconnected; as more personal information is processed or stored, the more effective security measures are required. In this presentation, attendees will learn about some fundamentals of these data privacy laws and how they relate to cybersecurity.

Making My Way Through Tech as a Neurodivergent, Queer, Woman of Color

Ruchira Pokhriyal

For LGBTQIA+ community in tech, it has been a long path to equality. Although leaders of some of the industry's most powerful players have come out, factors like workplace safety and acceptance are keeping many from fully expressing themselves. LGBTQIA+ individuals in tech face the challenge of being misgendered, having sexual orientation and gender presumed in the workplace, having identities invalidated, having pronouns disregarded and misused, and receiving anti-LGBTQIA+ comments or derogatory remarks. Coming out as LGBTQ at work is a prevalent issue, but there remain additional challenges once out, especially if someone is a neurodivergent woman and/or person of color. According to a demographics analysis from "Wired," Black, Latina and Native American tech professionals make up less than 5% of the workforce at major tech companies. People with neurodiversity are consistently underestimated for their knowledge and skills. In an increasingly progressive society, visibility for the LGBTQIA+, neurodivergent and women of color still remains highly overshadowed in tech. Through this lightning talk, the presenter aims to: empower the LGBTQIA+ community at WiCyS and tell them it's important to break through the shackles of confinement society has created and defy stereotypes, address people in leadership positions and help them understand that organizations should focus more on learning about communication styles and be more understanding of narrow social constructs because they limit a neurodiverse employee's potential for success, encourage women of color to be comfortable being uncomfortable and speak up, and encourage allies to use their skills and expertise to help other women in the field by giving them advice, introducing them to opportunities for jobs. Through

this lightning talk, the presenter aims to: 1. Empower the LGBTQIA+ community at WiCyS and tell them it's important to break through the shackles of confinement society has created and defy stereotypes. 2. Address people in leadership positions and help them understand that organizations should focus more on learning about communication styles and be more understanding of narrow social constructs because they limit a neurodiverse employee's potential for success. 3. Encourage women of color to be comfortable being uncomfortable and speak up. 4. Encourage allies to use their skills and expertise to help other women in the field by giving them advice, introducing them to opportunities or recommending them for jobs.

Cyber-Informed Engineering and the Future of OT Security

Cheri Caddy

Operational technology (OT) and control systems that operate power, transportation, water and pipeline systems are being increasingly automated, interconnected and virtualized. These trends are being driven by a continuing need to realize efficiencies and have been accelerated by the pandemic-inspired need for increased remote operation and by once-in-a-generation national investments (via the 2021 Bipartisan Infrastructure Law and the 2022 Inflation Reduction Act) in modernizing this critical infrastructure. Even as OT continues to converge with networked IT, exposing more of these systems to cyber risks, the engineers that design, build and operate OT and control systems lack the resources needed to ensure these systems are secure and resilient. The congressionally directed 2022 National Cyber-Informed Engineering (CIE) Strategy offers a comprehensive approach to increasing the education, training, R&D, tools and body of knowledge available to engineers to enable them to advance security-by-design for control systems. This presentation will outline the five pillars of the CIE Strategy and provide an update on national implementation efforts across the government, academic, research and asset-owner communities. The session will conclude with a call to action on how interested participants can get involved in implementation efforts.

Woody Woodpecker's Cybersecurity Lessons From 1957

Camila Martins

Threat actors have always existed. They are often very creative, quickly finding new ways to exploit their targets and surprising defenders with their clever deeds. It seems like each time defenders address a vulnerability, a new one appears in an endless loop. In this lightning talk, attendees will watch snippets of Woody Woodpecker's "Box Car Bandit" episode from 1957, where a bandit and his horse try to hijack a train carrying valuable goods. Woody works tirelessly to keep the attackers at bay and protect the assets. This whimsical animated film will help generate conversations around cybersecurity threats, vulnerabilities, controls and

2023 WiCyS CONFERENCE

LIGHTNING TALKS

strategy. Participants will discuss themes such as data integrity and confidentiality, proactive and reactive controls, incident response detection, containment and eradication, logging and alerting, honeypots and more. Woody Woodpecker's skills as a 1957 train guard would translate well into the Information Age and help address several cybersecurity challenges that organizations face today. Join this session for a fun and outside-the-box discussion on cybersecurity best practices and how to keep up with the ever-changing threat landscape.

LIGHTNING TALKS

SATURDAY • 11:00AM - 11:45AM

All Talks are in Room: Adams D

Track(s):  **CPE Credits: 0.75**

Real Talk: How to Navigate and Advocate as a Working Mom in Security Professions

Kavitha Sivagnanam

Despite modest gains in representation of women in technology and the cybersecurity sector over the last decade, women are dramatically underrepresented in executive leadership positions in corporate America. Research says only one in four C-suite leaders is a woman, and only one in 20 is a woman from certain ethnic groups. For every 100 men promoted from entry level to manager, only 87 women are promoted. As a result, men significantly outnumber women at the manager level, and women can never catch up. As the years progress, what is holding women back from getting promoted into senior leadership positions? Life happens! A woman also can become a mother. Women at all levels are far more likely than men to be responsible for most or all of their family's housework and caregiving. The imbalance is especially stark in certain ethnic groups. Despite being ambitious, the working mother's guilt held the presenter back at work for a long time. Someone else can do the job in the office, but there is no one who can do the work as a mom. The problem is profound in the security industry, where it's hard to find another female, let alone a working mother, who can be a mentor or a friend. The presenter will share some challenges she faced and how she learned to navigate this challenging field.

We Are the 82% - The Value of Securing the Human Element Through Cybersecurity Awareness and Training

Julie Marquez

People are the most critical aspect of security. According to the 2022 Verizon Data Breach Investigations Report, 82% of breaches involved the human element. Whether it is a phishing attempt or other social engineering methods with or without stolen credentials or just simply an error, people play

a large part in security breaches. To mitigate the risk human error introduces into organizations, people must have solid security awareness and training. A strong training program shares cybersecurity knowledge with employees by ensuring the workforce can spot and avoid cybersecurity threats, providing best practices to model appropriate cybersecurity behaviors and offering compliance and role-based skills security training. Bad actors are sticking with their favorite social engineering attack - phishing. However, smishing (a type of phishing message sent via text/sms message), impersonation with spear phishing and smishing, vishing (voice calls) and quishing (QR code) are on the rise. If the bad actors are upping their game, then awareness teams must do the same. This team becomes a critical line of defense offering the tools and education necessary for employees to recognize the fear and emotion embedded in these attacks so they think twice before clicking. Education and vigilance among employees becomes the best defense against these types of attacks. To properly secure a company, they must take a human-centric approach, which is no small undertaking. Make sure the security awareness and training team has a solid phishing program, create social engineering materials, and develop training that provides the necessary security skills for product teams to create secure solutions for customers. Companies must upskill the employee base, drive behavior change and reinforce good security practices. It will have to be repeated because this is about changing human behavior, which takes time and effort to mitigate risk to employees and the company. But this security expertise should also be shared with family, friends and the broader community.

Wait! They Said What? Hide Age and Years of Experience!

Deborah Kariuki

In this lightning talk, presenters will discuss the existence of gendered ageism and its negative impact on the careers of professional women. The misguided advice given to many women to scrap when they graduated from school, their years of work experience and/or age from their resume is demeaning. Why should older professional women have to diminish their true experiences? Sexism and ageism are real, and it cannot continue to be swept under the rug. In today's world, gender, race and age-based biases are a reality for most women. In some instances, hiring managers outwardly display these three biases during the recruitment process. The cybersecurity workforce is in need of both diversity and inclusion. Yet, nearly one-third of older women are unemployed and cite age discrimination as an impediment to finding a job. When cybercriminals carry out cyberattacks, they do not do so based on age discrimination; they are in fact equal opportunity perpetrators. Gendered ageism brings up the question of why older men are disproportionately valued over older women. Both groups have a strong work ethic, established professional networks, are more settled in life, and have often successfully weathered their fair share of life storms. Listen to this lightning talk as presenters tackle this issue of gendered ageism with specific emphasis on women in cybersecurity, and commit to continuing this discussion and implementing changes across organizations.

2023 WiCyS CONFERENCE

LIGHTNING TALKS

The Skills I Needed to Succeed in Cybersecurity I Learned in Kindergarten

Debby Briggs

During grade school, students are taught some of the most basic principles for success in life: don't talk to strangers, pick up, mind manners, watch for traffic, etc. For a long and impactful career in cybersecurity, many of the same principles surprisingly still apply. Phishing scams can usually be avoided with a little extra scrutiny of incoming messages, for example. Password maintenance is likewise a matter of routine cybersecurity hygiene. And while technical skills are needed for a job in cybersecurity, it's the soft skills involved in collaboration and strategic thinking that are often the most important when advancing in the business world, particularly for more senior roles. Sharing a few simple lessons learned in kindergarten, the presenter will relate how common sense principles and childhood skills many take for granted hold the key to a successful career in cybersecurity.

It Takes a Village: A Case Study in Securing Electoral Landscapes

Jolie Grace Wareham

Cybersecurity has only recently entered the everyday vernacular. The 2016 U.S. presidential election was the moment that turned many heads toward cyber concerns. Despite this, there is little being done to engage electoral communities in defending against cyberattacks. Campaigns and political parties across the ideological spectrum are on the receiving end of many threat actors' efforts. When electoral communities are not strategically included in conversations and efforts around cybersecurity, a serious blind spot emerges for U.S. national security. While government agencies have many essential efforts underway to secure voting processes and regularly publish advisories about electoral vulnerabilities, more needs to take place to build relationships and communication pathways between government stakeholders, cybersecurity professionals and electoral players (candidates, operatives, vendors, party officials, elected leaders and volunteers). Campaigns are often only as secure as the most tech savvy member of the campaign team and have no understanding of whether every volunteer with whom they entrust voter data practices cyber hygiene. Political parties have only recently begun building security teams and strategy, and these efforts often long for connectivity to government agencies and industry subject matter expertise that can assist in building long-term strategy infused with the NIST Framework and other industry standards. In order to have a more complete understanding of the threats the electoral sector faces, the country needs strong reporting structures between campaigns, political party organizations at all levels and government agencies. To demonstrate the potential of greater cross-sector collaboration around electoral cybersecurity, this talk will examine the work of the Tennessee Democratic Party Cyber Safety Committee (TNDP CSC). This is a standing committee of the Tennessee Democratic Party State Executive Committee as of 2021 and conducts vulnerability assessments and training, crafts policies and procedures aligned with the NIST Framework, and works to construct communication and reporting pathways with government stakeholders. This committee seeks to break down partisan and sector barriers, tirelessly working to identify thought and action partners across the aisle and in government agencies, legislative bodies and various industries. This talk also will explore the foundation and philosophy of the committee, as well as how its portfolio and vision has grown since its inception, and inspire attendees to share their experiences with cross-sector collaboration and electoral vulnerabilities. Attendees will walk away with a stronger understanding of how everyone must collaborate to dismantle silos, challenge the status quo and secure the electoral landscape.

2023 WiCyS CONFERENCE

LIGHTNING TALKS

Wandering the Wizarding World - Cybersecurity Concepts Through Harry Potter

Ann-Marie Horcher

Security usability is a complex topic of critical importance to any computer user, which can be almost anyone. Examples illustrating security usability concepts from a well-known and well-loved literary source like Harry Potter enhance both recognition and retention. Traditionally, people have learned life lessons from fables, fairy tales, parables and even urban legends. The ubiquity and popularity of the wizarding world of Harry Potter makes it a highly accessible source to mine for security usability education. Cybersecurity education is not a one-time action. Like safety procedures, it must be continually renewed to retain effectiveness. As stated in Carnot's second law of thermodynamics, a closed system trends toward entropy. To reverse this process, energy must be applied to the system. Similarly, to retain a state of cybersecurity awareness, energy in the form of innovative and engaging cybersecurity awareness training/education must be applied to thwart the trend toward entropy. This experience will give participants the opportunity to wander a 360-degree panoramic map of the wizarding world to learn crucial cybersecurity concepts. At each station, the participant will see a concept and example illustrated from Harry Potter then take a brief assessment to check their understanding of the concept.

Full Speed Ahead: Accelerating the DoD's Dominance with Cloud Native Security

Caitlin Delmore

The Department of Defense (DoD) is transforming how it delivers warfighter capabilities via the cloud. With a strong push for digital transformation, the DoD is aggressively working to modernize software practices to deliver resilient software at relevant speed. With various digital transformation and modernization strategies released, DoD entities are specifically using the cloud for enablement of software modernization. Although the DoD is working tirelessly to create various software factories and trusted software ecosystems, its efforts are at times siloed and face many roadblocks. The presenter will discuss where the Cloud Native Security Digital Transformation is today in the DoD, explain the DevSecOps practice, and discuss important software vulnerabilities that most commonly affect DevSecOps continuous integration/continuous delivery (CI/CD) pipelines in cloud native application security environments. They will explain common tooling seen in cloud native environments and how these tools expedite software delivery times. Then they will detail the high-level roadblocks the DoD is facing and propose solutions for how it can move forward with greater speed and increased security. The presentation will end with a high-level roadmap of where the DoD is heading and where it is asking for industry help/support. The presenter will engage the younger audience members by capitalizing on the capacity for growth career-wise within cloud security.

Exploring Systems Thinking Through Gamification for Cybersecurity Training and Education

Olivia Schmidt and Alison Owens

People begin playing games in early childhood and continue playing them throughout their lives. These games, whether digital or analog, engage individuals physically and/or mentally at home or elsewhere. Some games focus more on universal patterns of recognition while others are designed for a specific culture. However, almost all games are environments that function as larger systems, model real-world interconnections and contain microcosms for learning. In these structured playing environments, players acclimate to their surroundings and develop certain mindsets for how gameworld objects interact and fit together. In the cybersecurity realm, software games have been used to increase employee awareness while gamified exercises like capture the flag (CTF) are used to test players' cybersecurity skills. For both of these applications, games or game elements were used as exercises in systems thinking. Players are encouraged to think about relationships rather than isolated information and give thought to how their actions might be influential or impact the actions of other players/AI who are attacking them. This mode of thinking, to analyze how parts of a whole interact to produce an outcome, supports systems thinking and the status of games as rule-based, dynamic systems of learning. While the rules of cyberspace are different from the physical world, the video game realm offers a unique bridge between both; it is a space where players can take real-world models and experiment in a safe, inconsequential environment to try to understand and tackle the unpredictable outside world. This talk will discuss how games and their elements are ideal mechanisms for solving real-world cybersecurity problems and deliver complex system design models as well as best practices for designing gamified learning environments that accomplish systems thinking.

2023 WiCyS CONFERENCE

CAREER VILLAGE TALKS

THURSDAY CAREER VILLAGE TALKS

All Talks are in Cottonwood 2

CybHER DivHERsity - Hacking the Glass Ceiling

Time: 2:00pm - 2:30pm

Perri Nejib, Dawn Beyer and Smruthi Sandhanam

This talk will explore multiple perspectives on diversity within the cyber career field. Comprised of a diverse group of women cyber professionals, each will offer their unique skills, knowledge, backgrounds, and experiences that have shaped them towards their current careers in cyber. Diversity plays a critical role in technical innovation and agility, and technical diversity is a key component in the field of cybersecurity. The speakers have been specifically chosen to reflect underrepresented groups as well as those at different stages of their career to provide multiple perspectives on the topic of diversity in cybersecurity.

I Got Your Back: The Importance of Mentors and Sponsors

Time: 2:30pm - 3:00pm

Lisa McKee, Lynn Dohm, Veronica Doak and Nakia Grayson

Once women enter the workforce, climbing the corporate ladder can be challenging. Approximately 25% of the security workforce is women and a small subset are in leadership. This session, we will discuss the differences between mentors and sponsors, how to find the right person to support you on your career journey, and what it means to continue having other women's backs as they make their way into senior roles. Share success stories from a mentor and her mentees.

The Career Path is a Road Trip

Time: 3:00pm - 3:30pm

Tonia Dudley

Navigating a career change can be intimidating. Where do you start? How do you shift from one profession to another? Having traveled from Finance to IT to InfoSec, this talk will provide insight into ways to make a career change and leverage your current employer.

Producing a Personal Brand

Time: 3:30pm - 4:00pm

Lisa McKee

A personal brand defines how you speak to the world, and if you are applying for a job, starting a company, or establishing yourself in the field of cybersecurity, this branding speaks volumes. Participants will learn the benefits of personal branding, strategies for creating a brand, and step by step instructions for how to live the brand and leave a legacy for others to follow. It includes practical guidance for knowing your audience, developing a social media presence, and growing your network, while maintaining a work-life integration.

The Marvelous Map of Cybersecurity Domains

Time: 4:00pm - 4:30pm

Rachael Klammo Crowthers and Fatemeh Ebrahimi

So, you're interested in cybersecurity but don't know the best place to fit in. Well look no further than the Map of Cybersecurity Domains! In this talk, we will review the Map of Cybersecurity domains with active participant discussions digging into what it really means to be interested in Cybersecurity. We're going to dive into some of the lesser advertised roles and show you what a day to day looks like and how you can get started. Our goal is to demonstrate to our audience, novice or experts, tech savvy or not, there is a home for everyone in cyber.

Navigating the Social Media Landscape

Time: 4:30pm - 5:00pm

Ashley Mahoney

Giving attendees information about how to appropriately present themselves on social media to help their careers. This is beneficial because the impact of social media can help or hurt career goals. It can mean getting a job or losing a job with the wrong content posted. Clear language and examples will be used that participants can immediately apply, adjust, and start to change how they present themselves online. This can lead to better chances at employment and a better professional appearance.

2023 WiCyS CONFERENCE

CAREER VILLAGE TALKS

FRIDAY CAREER VILLAGE TALKS

All Talks are in Cottonwood 2

Hacking into Cybersecurity Careers

Time: 9:45am - 10:15am

Julia Costin

Recent McKinsey research indicates the global cybersecurity market will grow to nearly \$2 trillion -10 to 15 times current spending across the business spectrum. High demand for cybersecurity talent – technicians, technologists and innovators – is clear. In 2023, cybersecurity remains a top priority for businesses, as they strive to maintain a balance between in-office and remote work. The frequency of cyber-attacks is relentless, and this is driving a constant demand for cybersecurity professionals with no signs of slowing down. For those aspiring to progress their careers in cybersecurity or make a start in the industry, acquiring cybersecurity certifications can increase the chances of securing employment, enhance careers, and safeguard against job loss during economic downturns.

CyberSecurity Leadership Sudoku

Time: 10:15am - 10:45am

Toby Liftee, Marti Mondragon and Bryn Preuss

Leaders come in various shapes and sizes, cultures and genders, that possess many qualities that can shape the course of a person's career. Whether you are early-in-career, leading a team or ready to reassess a career change, this discussion will provide some tips or guidance on where you may focus, plan and take actionable steps. Join this informal, fun Sudoku-like interactive session as presenters share 9 key leadership qualities that can intertwine and apply towards any Cybersecurity career journey.

Paradox of Career Advice: How to Build a Balanced Life

Time: 10:45am - 11:15am

Lauren Strobe

There is an immeasurable amount of conflicting and unrelatable career advice today. TikTok tells us to be a corporate girl, but Reddit tells us to unionize. We should be leaning in, but also starting a side hustle. As a self-described career-help junkie, I've seen the videos, read the books, and listened to the podcasts. This talk will present what worked for me, what didn't, and more importantly how I sifted through it all to create a life I want to live in.

Imposter Syndrome: Making It Without Faking It

Time: 11:15am - 11:45am

Ossie Munroe

Feelings of not belonging often stem from insecurities and sometimes from unfounded external pressures. Building confidence, staying true to yourself, and focusing only on things you can control are all tools available to combat imposter syndrome.

MID-CAREER BREAKFAST

The Mid-Career breakfast is a place for mid-career professionals to meet up, make connections, talk about the challenges faced by mid-career cyber talent and brainstorm ideas to help encourage and engage other mid-career professionals.

Sponsored by:

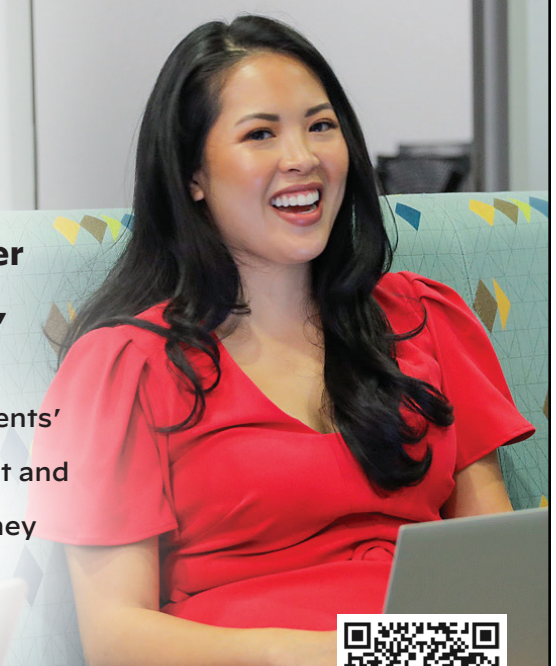


Located in Juniper B
Friday • 7:00am - 8:15am

*This event is by invitation only
and not open to all attendees!
RSVP is required.*



We aim to be the best company you will ever work for. We do this by putting people first, providing choices whenever possible, and recognizing that each employee is a unique individual. To be our clients' best cybersecurity partner, we recruit exceptional talent and help employees on their growth and development journey in ways that are individually meaningful.



FOLLOW US AND LEARN MORE ABOUT #LIFEATPALOALTONETWORKS

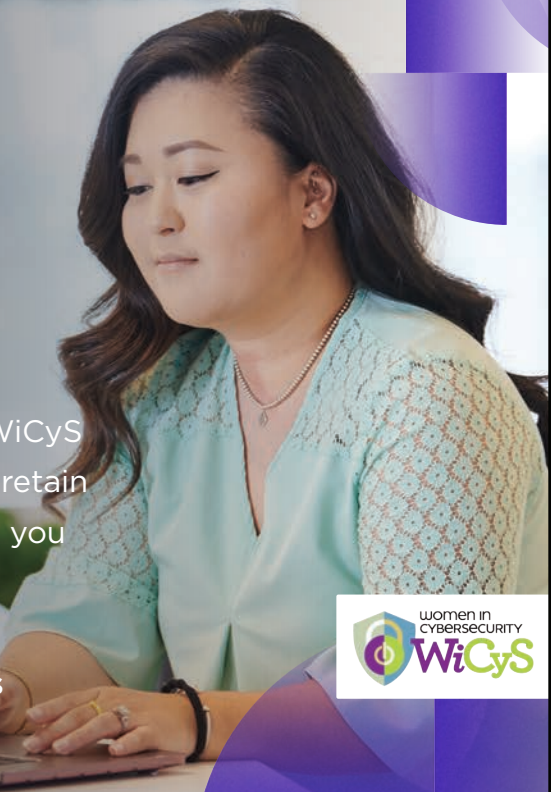
  @LifeAtPaloAltoNetworks |  @WeHireLeaders |  Palo Alto Networks



Protect the world with us

SentinelOne is a proud platinum sponsor of the WiCyS 2023 Conference as we work together to recruit, retain and advance women in Cybersecurity! Love what you do and work with the best minds in the industry.

Check out our openings at sentinelone.com/jobs



2023 WiCyS CONFERENCE

STUDENT POSTERS

STUDENT POSTERS

FRIDAY • 9:45AM - 11:00AM

All Student Posters are outside Aurora Ballroom & Exhibit Hall

1. An Efficient Traffic Analysis-Based Drone Detection Approach Using Deep-Learning Models

Masoumeh Abolfathi and Jafar Haadi Jafarian; University of Colorado Denver

Drones, also known as unmanned aerial vehicles (UAVs), are rapidly gaining popularity due to their decreasing costs and alluring features. Indeed, they are already being used for a variety of functions, including inspections, perimeter security, remote monitoring and emergencies. Although drones offer many advantages, they also might be used for malicious purposes, such as violating limited access zones, taking video or pictures of them, recording audio, live streaming, hacking WiFi-enabled devices to infer sensitive data, or even affecting critical infrastructures like airports and industrial sites. There is a big demand for a novel and effective drone-detection mechanism. There are four key tactics for drone detection: 1) visual detection; 2) audio detection; 3) radar detection, and 4) RF detection. These existing approaches require specialized hardware, however, the literature still lacks an affordable and effective solution that enables the recognition of a drone's presence in an area. PiNcH is the state-of-the-art drone-detection method that uses the intercepted communication traffic between the drone and its remote controller (RC). It employs random forest as a classifier. This research paper aims to leverage the power of pure data driven deep-learning models, including CNN, LSTM, bidirectional LSTM, GRU, and CNN + BiLSTM and their unique characteristics in automatic feature extraction to classify the encrypted packets based on unencryptable features such as packet size and timing. These models detect drones sent/controlled by an adversary. The train/test data split was done as follows: 70% of the samples were reserved for training, 20% for validation, and the other 10% for test. The experiments in this work were developed in Python 3.6 using Tensorflow to develop neural network models, and Keras-Tuner was used to perform automated hyperparameter tuning. The experimental results demonstrate that the proposed approach can achieve an accuracy of more than 94% to identify the drone's presence in a variety of heterogeneous circumstances that outperform PiNcH.

2. Detecting and Distinguishing Malicious Computer Network Traffic Using Machine Learning

Jerry Adams; Chaminade University of Honolulu

Computer network intrusion cyber attacks have become more widespread and of great concern for IT professionals and corporate leadership alike. Unauthorized intrusions are usually mitigated using intrusion detection systems (IDS), a computer network device that monitors and controls incoming and outgoing network traffic data. However, traditional IDS rely on known malware signatures, therefore limiting their detection of new or unknown malware. This project sought to overcome this problem by applying statistical models and machine-learning algorithms to distinguish anomalous patterns in the data, therefore identifying malicious network traffic as it passes through the IDS. The methods used were the testing and training of three statistical models: Random Forest, Decision Tree and Naive Bayes using a publicly available data set that simulated malicious traffic flow on a modern corporate network. The results support the hypothesis that using statistical models and algorithms is a valid way to classify a data set of network traffic to distinguish between normal and malicious network traffic. The accuracy of the models to distinguish malicious network traffic ranged from 62% to 89% accuracy. The false-positive rates of all models were <1%, which is ideal. However, the true positive rates for all three models were below 60%, with the worst performing model at a mere 30% true positive rate. Future work includes running other statistical models or machine-learning algorithms on the data set to determine if these models return more accurate scores and results for detecting malicious network traffic.

3. A URL-Based Social Semantic Attacks Detection with Character-Aware Language Model

May Almousa and Mohd Anwar; North Carolina A&T State University

Social engineering attacks rely on human errors and behavioral choices. The semantic attack, a subcategory of social engineering attacks, uses behavioral or cosmetic deception vectors (e.g., attacker creates a malicious website that looks and behaves like the legitimate one). The most common types of social semantic attacks include phishing, spamming, defacement and malware. We investigate the feasibility of developing URL-based social semantic attack-detection models using character-aware language models. Specifically, we developed three types of models: Long Short-Term Memory (LSTM)-based detection model, convolutional neural network (CNN)-based detection model and CharacterBERT-based detection model. Using the CharacterBERT-based detection model, the overall evaluation recorded a high detection accuracy of 99.65% by averaging the results of performing a five-fold cross validation. Considering the model performance per class, the CharacterBERT model ranked the best model among our three in detecting the social semantic attacks, reaching best accuracy of 99.90% in detecting a defacement attack.

2023 WiCyS CONFERENCE

STUDENT POSTERS

4. Cryptocurrency Prices Analysis Via Long Short-Term Memory

Melissa Amenuveve and Hongmei Chi; Florida A&M University

Cryptocurrency is a digital currency that uses a decentralized system – a blockchain – to record transactions and issue new units. Just like standard currencies, the value or prices of these fluctuate heavily and depend on a few variables. The crypto industry is very lucrative, and careful investments in cryptocurrencies such as Bitcoin (BTC), Ethereum (ETH), Dogecoin (DOGE) and Cardano (ADA) have created overnight millionaires. Cryptocurrency also is a favorite target for cybercriminals, hackers and fraudsters. Many government bodies regulate cryptocurrency, but there is no unified framework. This regulatory wiggle room allows crypto businesses to experiment and grow quickly, but it also means that risky practices that expose consumers can go unchecked. Using machine-learning methods with past prices as training data, we can predict future prices through time series forecasting, which can be crucial for investors in the market. In this study, Long Short-Term Memory (LSTM), a recurrent neural network (RNN) algorithm, will be used to analyze and make predictions based on previous pricing data. We also will describe the techniques applied to find the most suitable LSTM model parameters and the methods involved in predicting cryptocurrency prices using the algorithm. Preliminary results will be reported in this poster.

5. Gadgets of Gadgets in Industrial Control Systems: Return Oriented Programming Attacks on PLCs

Adeen Ayub, Irfan Ahmed and Wooyeon Jo; Virginia Commonwealth University, Nauman Zubair and Hyungkuk Yoo; The University of New Orleans

In industrial control systems (ICS), programmable logic controllers (PLC) directly control and monitor physical processes in real-time, such as nuclear plants and power grid stations. Adversaries typically transfer malicious control logic to PLCs over the network to sabotage a physical process. These control logic attacks are well-understood as containing machine instructions in network packets and are likely to be detected by network intrusion detection systems. On the other hand, return-oriented programming (ROP) reuses blocks (or gadgets) of existing code in computer memory to create and execute malicious code. It limits or eliminates the need to transfer machine instructions over the network, making it stealthier. Currently, ROP attacks on control logic have never been discussed in the literature to explore it as a practical ICS attack. This paper is the first attempt in this direction to explore challenges for a successful ROP attack on real-world PLCs, including maintaining a continuous (control logic) scan cycle through ROP gadgets, no user input (to cause a buffer overflow) to overwrite the stack for gadget installation, and limited ROP gadgets in a PLC memory to find blocks of instructions equivalent to the high-level constructs of PLC programming languages (such as instruction list and ladder logic). We identify and use typical PLC design features

(that we find exploitable) to overcome these challenges, which makes ROP attacks applicable to most PLCs, e.g., no stack protection and remote access to certain PLC memory regions via ICS protocols. We demonstrate two successful ROP attacks on the control-logic programs of three fully functional physical processes, i.e., a gas pipeline, a belt conveyor system and a four-floor elevator. The first ROP attack manipulates a PLC's current control logic and has two variants involving either single or multiple gadgets; the second ROP attack constructs a control logic from scratch using gadgets in a PLC's memory. Our evaluation results show the attacks can be performed using small-sized (2 to 4 bytes) gadgets with no significant effect on a PLC scan time.

6. Design and Implementation of GapApp

Callie Balut, Dr. Rachelle Heller and Dr. Costis Toregas; George Washington University

This research poster describes the follow-up to a CySP capacity-building project. GapApp is an application based on the outcome recommendations of the May 2021 Closing the Gap: Reentry of Women Veterans into Cybersecurity Careers conference. Of the three key observations from the conference, one noted a wealth of information and resources available to help women veterans. This observation led the research team to consider developing an accessible application for reaching these resources for the target audience: women veterans. All military work roles are codified in Military Occupational Specialties (MOS). The National Institute of Standards and Technology (NIST) has worked to codify the careers and positions within the National Initiative for Cybersecurity Education (NICE). However, the terms do not reflect each other. For our app, we manually compared each NICE task with our database descriptions of each MOS and assigned task IDs to those that best matched the MOS. GapApp permits users to indicate their MOS and be guided to a list of related cyber careers.

7. Forensic Analysis of Two-Factor Authentication Applications

Jessica Berrios, Elias Mosher and Sankofa Benzo; University of New Haven

With the fast-growing population of malicious attacks occurring every day, security is becoming increasingly difficult to ensure. The most common attacks many users and large corporations fall victim to are phishing attacks, spear phishing, keyloggers and credential stuffing. This is where two-factor authentication (2FA) comes in, as it can help in preventing bad actors from accessing personal and professional accounts. Companies are realizing the need for 2FA, as it can help prevent attacks that can result in the loss of millions of dollars from stolen data. Many institutions such as banking, academics, health care and others are making 2FA mandatory for all their registered users. The growth of users implementing 2FA demonstrates an important forensic need to understand how these applications operate and what kind of information they store. The research presented here focuses on analyzing 10 popular 2FA applications and

2023 WiCyS CONFERENCE

STUDENT POSTERS

the digital artifacts left behind. Our analysis includes Aegis, FreeOTP, Google Authenticator, Microsoft Authenticator, TOPT Authenticator, 2FAS Authenticator, Twilio Authy, KeePassXC and OTP Authenticator. The devices used to perform this research included a Samsung Galaxy S6 (Android 7), an iPhone 7 (iOS 14.7.1) and a Windows 10 virtual machine. The methodology consisted of four phases, which included the creation and setup of the accounts and devices. The 2FA applications were then tested on five applications, which included Facebook, Twitter, Dropbox, Snapchat and Instagram. In order to generate more data, network traffic also was acquired. During the analysis phase, researchers meticulously analyzed all information acquired from the images off the phones, network traffic, and memory and disc image acquired from the Windows machine. The results revealed that a majority of the applications store unencrypted information such as secret keys, timestamps and account information that include an issuer name, email and 2FA passwords. A security vulnerability was discovered that allows for TOTP codes to be regenerated on another device using the secret keys obtained. This allowed researchers to gain access to accounts that have 2FA activated without the need to have the original device available. Finally, to assist in the analysis of relevant information we share a tool that aids the automatic extracting of forensic artifacts. The tool will present the forensically relevant data when it is presented with the forensic image of a mobile device.

8. A Framework for Identifying Malware Threat Distribution on the Dark Web

Shelby Caldwell and J Todd McDonald; University of South Alabama

The dark web is an ever-growing phenomenon that has not been deeply explored. Contents of the dark web are primarily the buying and selling of unauthorized goods, illegal activity and trading services. It is no secret that in recent years, malware has become a potent threat to technology users. Cybercriminals and hackers utilize the dark web for malware distribution by selling the code under aliases and via cryptocurrency. The dark web is known for supporting anonymity and secure connections for private interactions, thus making it a favored medium for people who engage in illegal activity, a rich environment for discovering trends, details and indicators of emerging malware threats. By examining this malware threat distribution, we gained useful information regarding this activity. Through the application of data science and open-source intelligence techniques, trends in malware distribution can be studied, such as the types of people selling the malware, the amount of malware being exchanged, the type of currency being used, and what malware is gaining popularity at a specific time. This information aids law enforcement, researchers and businesses in pursuit of mitigating the risk and containing the spread of malware. In this research, we aim to create a framework for helping identify malware threat distribution patterns. We examine this type of dark web activity using an automated and manual approach that collects data on malware exchanges. The automated approach will include spidering techniques and machine learning algorithms to determine

characteristics of malicious software. The manual approach will be a more tedious procedure, which will involve tracking specific steps and documenting the journey of obtaining malware. Furthermore, a comparative analysis is conducted to determine which approach is more effective and efficient. Our framework for identifying current or future malware threats distributed on the dark web will be refined by examining the weaknesses and strengths of each gathering approach.

9. DLPA on a Hardware Implementation of GIFT-COFB

Cassi Chen; University of California, Berkeley, Michel Liao; Timberline High School, Paul Vanderveen, Liljana Babinkostova, Edoardo Serra and Aparna Sankaran; Boise State University

With the expansion of the Internet of Things (IoT), concerns about security measures on resource-constrained devices susceptible to side-channel attacks (SCA) have been raised. In 2016, The National Institute for Standard and Technology (NIST) initiated a process to evaluate lightweight cryptographic (LWC) algorithms for lightweight devices where current NIST cryptographic standards perform poorly. This research investigates side-channel vulnerabilities of unmasked and masked versions of GIFT, one of the 10 NIST lightweight cryptographic algorithms finalists. To test the resilience of GIFT against SCA, we apply Deep Learning Power Analysis (DLPA) to its hardware implementation.

10. Detection of Cyberbullying in GIF/Stickers Using AI

Pal Dave; North Carolina A&T State University

Cyberbullying is a well-known social issue, escalating every day. It can be done intentionally or not by social media users. It can be unintentional because sometimes a user might not know what it means, but they use it out of curiosity or without being concerned. Research has shown most adolescents are more involved in cyberbullying associated with social media because of a lack of knowledge and understanding. Cyberbullying also can be done using text messages, images, speech and even GIFs, which can be stickers, animation-based images or a very short video. Nowadays, using stickers is one of the most popular ways to communicate with each other, which helps people post their opinions, expressions or thoughts on social media. It has been predicted that users send 380 million stickers and GIFs each day on social media, and their usage will grow greatly in the near future. Machine-learning methods have been developed to detect cyberbullying in text and images, however, there are only a few studies available for detecting cyberbullying in GIFs. The goal of this research is to detect cyberbullying in GIFs, which helps the safe use of the social medium and promotes awareness related to cyberbullying in adolescents and for all social media users. We propose using Convolutional Neuron Network-based deep learning models to detect this type of cyberbullying. We will collect the dataset and train deep-learning models such as VGG16, GoogleNet, LeNet, AlexNet, etc. and compare the performance of these models.

2023 WiCyS CONFERENCE

STUDENT POSTERS

11. A Deep Learning Approach for Intrusion Detection in Internet of Things Using Focal Loss Function

Ayesha Dina, Muhammad Abu Bakar Siddique and Dakshnamoorthy Manivannan; University of Kentucky

Internet of Things (IoT) is likely to revolutionize healthcare, energy, education, transportation, manufacturing, military, agriculture and other industries. However, for the successful deployment of IoT in various industries, methods for detecting and preventing security breaches need to be designed and implemented. Over the past decade, a number of researchers in academia and industry have used machine learning (ML) techniques to design and implement Intrusion Detection Systems (IDS) for computer networks in general; however, not much work has been done for intrusion detection in IoT. Datasets collected by various organizations were used by many of these researchers to train ML models for predicting intrusions. It is common for datasets used in such systems to be imbalanced (i.e., not all classes have equal number of samples). Predictive models developed using ML algorithms can produce unsatisfactory results if imbalanced datasets are used for training the models. Techniques such as random oversampling and undersampling do not produce robust models. Furthermore, ML models trained using traditional loss functions, such as cross-entropy loss, fail to accurately predict minority class instances. To overcome the data imbalance problem for intrusion detection in IoT, we leverage the specialized loss function, called focal loss, that automatically down weights easy examples and focuses on the hard negatives by facilitating dynamically scaled-gradient updates for training effective ML models. We implemented our approach using two well-known deep learning (DL) neural network architectures. We conducted extensive experimental evaluations using three datasets from diverse IoT domains and compared our proposed approach with state-of-the-art intrusion detection models. We found that our approach (training DL models using focal loss function) performed better with respect to accuracy, precision, F1 score and MCC score by as much as 24, 39, 39 and 60, respectively, compared to training them on the datasets using cross-entropy loss function. Our approach also performed better compared to other state-of-the-art approaches.

12. Autonomous Intelligent Cyber Defense with Cognitive Models

Yinuo Du, Baptiste Prebot and Cleotilde Gonzalez; Carnegie Mellon University

To support the future cyber battlefield, many technological advances are required in the proposed architecture of autonomous intelligent cyber defense agents (AICA). In particular, AICA's decision-making processes will need to be dynamic and adaptive to the actions of intelligent attackers. AICA's decision-making algorithms must rely on theories that formalize dynamic decision processes; decisions made from experience; and the capabilities to learn, adapt and react in the face of uncertainty. During the past decade, researchers of behavioral cybersecurity have created cognitive agents able to learn and make decisions in dynamic environments in ways that assimilate human decision processes. However, many of these efforts have been limited to simple detection tasks and represent basic cognitive functions rather than a whole set of cognitive capabilities required in dynamic cyber defense scenarios. This poster will introduce our work on the development of cognitive agents that learn and make dynamic defense decisions during cyberattacks. The cognitive models are trained in a simulated environment that relies on OpenAI Gym and Cyborg, adapted from an existing CAGE scenario. The capability of these agents is evaluated in a Turing-like experiment, which compares the decisions and performance of these agents against human cyber defenders. We will present an initial demonstration of the cognitive model of defenders that relies on a cognitive theory of dynamic decision making and Instance-Based Learning (IBL) Theory. The poster also will feature a new interactive defense game, where human defenders can perform the same CAGE scenario simulated with the IBL model. Through computational modeling and human-subject experimenting, we highlight the potential of cognitive models in adversarial cyber scenarios, which can capture the behavior of humans involved. This work will provide insights on the cognitive foundations required to build AICA with recommendations for how to make better artificial intelligent agents that share mental models and collaborate better with human operators in cyber defense teams.

2023 WiCyS CONFERENCE STUDENT POSTERS

13. Forensic Evaluation of Roku Streaming Stick 4K

Kyla Fielding; Norwich University

Internet of Things (IoT) devices are products with various smart capabilities that allow users to perform tasks on a network. There are thousands of devices in the market with smart attributes, and by 2025 there is expected to be over 82 billion devices connected to the internet. Streaming devices give an individual the ability to watch streaming channels, play games and cast movies. This research aims to forensically analyze the most popular model, the Roku Streaming Stick 4K (known as Maddison), and its respective mobile application, Roku Remote, on a Pixel 2 to identify artifacts that would be useful to the forensics community. This poster presents the analysis of network activity produced by the device, extraction of information from debugging channels and brightscript tools offered through development mode, and assessment of the free mobile remote application. This paper also talks about the challenges associated with these techniques such as issues with brightscript language and navigating the file system.

14. EEG-MFA: One Step, Seamless Multi-Factor Authentication using EEG Signals

Sindhu Reddy Kalathur Gopal; University of Wyoming

Currently used multi-factor authentication (MFA) systems such as Pulse Secure, Duo Security, Okta, etc. are believed to enhance the security of users' accounts and data. These MFA applications, however, raise usability concerns such as users must go through an additional step to verify their identity. For example, the user must enter an OTP code or accept a push notification within the specified time. Traditionally used MFA systems are susceptible to security threats, such as phishing attacks, losing tokens and those on mobile devices. In order to overcome issues associated with MFA methods currently in use, we propose EEG-MFA, which validates the user unobtrusively without taking time off from work. Electroencephalogram (EEG)-MFA is a one-step, multi-factor authentication system that relies only on a familiarity factor in concealable EEG signals that are acquired while the user enters passwords to log into their systems. EEG-MFA mitigates impersonation attacks because EEG is concealable, unique to each individual and is resistant to spoofing attacks and identifies the user unobtrusively.

**Interested in trust and
security at scale?**

**Come talk to us at
WiCys 2023!**

shopify.com/careers



2023 WiCyS CONFERENCE

STUDENT POSTERS

15. Stopping Attackers in their Tracks: Attacker Actions Lead to Memory Corruption in Exploit Scripts

Rezvan Mahdavi Hezaveh, Md Rayhanur Rahman and Laurie Williams; North Carolina State University and Shane Fry, Doug Britton; RunSafe Security

One of the oldest questions in cybersecurity is “How good is a pound of cyber?” Governments, company chief information security officers and product manufacturers struggle with independent assessments of how effective their defenses are or how effective their products are in defending. This research study proposes an unbiased, scalable way of asserting the effectiveness of cyber protections called Attacker-Action Based Protection Measurement (AABPM) by benchmarking against exploits. Across the cyber industrial base, AABPM can change the game for measuring how completely companies or agencies have secured their borders and layered defenses against actual attacks. For AABPM, the first step was to create a comprehensive list of all the actions an attacker would take in a memory-corruption attack. The manual and iterative analysis of 6% of memory-corruption exploit scripts in the exploit-db website resulted in finding 40 actions, such as EIP overwrite (return address overwrite), using nop sled, writing outside the buffer and jump to ROP gadget. Since attackers perform several steps in an attack, each exploit script could have more than one action, for example, (1) adding some new content to memory and then (2) jumping into the new memory content. After determining the universe of actions, the next step was the creation of a natural language processing (NLP) model to parse the identified actions out of the 4,634 memory-corruption exploit scripts on the exploit-db website. The model was evaluated on 100 randomly selected exploit scripts by two reviewers. Our NLP model has 0.57 precision, 0.86 recall and 0.63 f1-score with weighted averaging on attacker action identifications. The initial demonstration of AABPM was done to help a cybersecurity company measure its product effectiveness at stopping all the memory-corruption based attacks. We worked with the company's security researchers to identify the indicia of each action, for example, what will overwrite EIP look like versus using a nopsled. The list of attacker actions was then grouped into those the company product would inhibit (e.g. jump to the ROP gadget) versus those the company product wouldn't inhibit (e.g. dereference null pointer). In the third step of AABPM, we consider that the company's product is effective against an exploit if at least one attacker action in the exploit is among the inhibited group because exploit scripts require successful execution of each action for it to work. In the previous example, if the product breaks adding new content to memory, the jump into new memory won't work. That allowed for the analysis of all 4,634 scripts to determine the effectiveness of the company's Runtime Application Security Protection (RASP) technology. Further work will include the following: 1. The creation of an enterprise scoring method. 2. Allowing the inclusion of binary-based exploits instead of just script-based. 3. Expanding actions to non-memory corruption-based scripts (e.g. command injection, SQL injection, directory traversal, etc). 4. Expanding to include other forms of attack delivery (e.g. email and text for phishing-based exploits, etc).

16. Machine Learning Trust Management System for Blockchain Organ Donation Framework

Ayushi Mehrotra; Troy High School

In 2022, there were about 105,800 patients waiting for an organ to survive, yet 17 of them die every day. Organ shortages have been an ongoing problem since the start of the organ donation process, and many optimizations to the system, such as Radio Frequency Identification (RFID) on cadavers, have been made to decrease the number of organs lost in the process. However, recently there has been a report by the Office of Inspector General (OIG) that outlines the security protocols in the Organ Procurement and Transplantation Network (OPTN), which reveals the lack of access controls, system monitoring, and written policies and procedures. The missing controls are used to assist in the detection of cybersecurity attacks and restrict access to terminated user accounts. If an actor is able to penetrate the system, like the ransomware attack on Midwest Transplant Network reported by KCUR, it could have devastating consequences for patients and organs. In this study, we will focus on preventing malicious nodes from entering the network and detecting internal attacks on the network. For the former, we propose a blockchain organ donation network using Hyperledger Fabric. Blockchains are distributed and ledgers shared for keeping unalterable records across the network. Records are added to the database through a consensus mechanism, such as Proof of Work (PoW) or Proof of Stake (PoS). With a blockchain organ donation system, it can prevent other nodes from entering the network and verify blocks being appended into the ledger. For detecting internal attacks, such as on-off attacks, we propose to integrate a machine learning-based trust management framework with the blockchain organ donation system. Trust management is the concept that uses social trust in a network to help decision making. By collecting data on interactions between the nodes and the reputation of nodes, machine-learning models are able to predict trustworthiness and maliciousness. With this identification, OPTN may initiate prevention protocols to stop an attack.

17. A Framework for Evaluating Security and Usability of Parental Controls in Streaming Services

Amanda Moctezuma and Stefan Robila; Montclair State University

Kids from 8 to 18 spend a daily average of 7.5 hours in front of a screen for entertainment purposes. According to the Kaiser Family Foundation, out of that time, 4.5 hours are spent watching, whether over the air or through one of the many streaming services. These days, we are surrounded by technology, and a significant amount of the population, including adolescents and children, has access to electronic devices. However, due to the broad knowledge containment, they have access to content that may be inappropriate for their age. To address this situation, parental controls can be placed on their devices. These are software services that allow people to monitor and restrict

2023 WiCyS CONFERENCE

STUDENT POSTERS

what another person does online. For content controls to be effective, they must rely on rigorous rating systems. In the U.S., online video content is rated using the television content rating system, a voluntary schema co-designed by content creator organizations and civil society groups and promoted by the Parental Guidelines Monitoring Board. Success in the adoption and use of such systems relies on adoption by content providers, public awareness, ease of use and reliability. Through this poster, we describe the development of an evaluation framework for parental controls as a mechanism for managing children's access to video content. While parental control applications have included a variety of online interactions such as web browsing, social network activity, etc., this project focuses on controls for video streaming service applications such as YouTube, Netflix, Prime and Disney+. The framework was designed with two components. In the first phase of this research, the differences, effectiveness, and the user's perception of various parental control software systems were investigated. This was done through surveys that evaluated both general aspects of controls as well as usability questionnaires focused on individual applications. Results from this phase indicate that while control mechanisms are seen as necessary, their usage continues to be low. Factors that limit their adoption include a limited understanding of their functionality, significant differences in the interface between various services, and a lack of hardened security. In the second phase, the goal was to further analyze the security and usability features placed into the parental controls of different streaming platforms and suggest ideas for improvement by building an evaluation toolkit grounded in previous literature as well as user feedback. The toolkit is formed on a set of evaluation criteria that includes user experience (ease of access, cross-platform availability, etc.), security (authentication mechanisms strength, ease to bypass controls, etc.), and alignment with the content rating system (and ease of customization of a content rating beyond a rigid system) for which scores are generated. The toolkit was used to evaluate the largest streaming services (by number of users). The results show that parental controls continue to be quite diverse in implementation across various platforms, leading to non-uniform experiences and limited usage, a concerning aspect given the continuous growth and diversification of the content-streaming industry.

18. Survey on Security, Privacy and Societal Implications of Using Augmented Reality and Virtual Reality in Education

Salome Pantuvo and Samantha Collen; Saint Cloud State University

Augmented reality (AR) and virtual reality (VR) are closely related but not the same technological fields. Both have emerged as powerful models in recent years. AR alters one's current perception of a real-world environment by adding digital elements - visual, auditory or sensory to a live view often via the camera on a smartphone. In contrast, VR replaces the real-world environment with a simulated one, experienced via a device such as a headset or goggles. The significantly noticeable difference between AR and VR is in the hardware device itself. With application domains across

all fields, the integration of AR and VR has the prospective to profoundly change the role that technology plays in our educational institutions' teaching and learning experience. Although these innovations enable users to interact with digital content in a new and stimulating way, AR and VR technologies also may expose users to new security, privacy and societal risks from the capabilities that make these technologies so influential. A deep understanding of these risks or vulnerabilities is currently unknown, nor is the preventive or definitive solution against these unknown risks available. This paper assessed the level of awareness of AR and VR among educators and students. The top two concerns raised by participants were the fear their phones could be remotely hijacked and tracked. About 37% of respondents raised these concerns with more educators (23) than students (9) expressing at least one of these misgivings. Surprisingly, health and safety concerns and privacy issues such as theft of users' credentials were not a worry to many of the participants.

19. Automated CWE-Vulnerability Prediction Using Abstract Syntax Tree Embeddings

Salome Perez; University of Nebraska, Lincoln

Nowadays, almost every aspect of our lives interacts with software and the security and privacy implications that come with it. As such, Java, one of the most prominent programming languages for building software, is challenged by a prolific number of bugs and vulnerabilities that remain latent and can result in massive exploits, such as the Log4Shell vulnerability in 2021 that compromised a massively used Java library for logging processes to allow remote code execution by attackers. The software security research community is actively looking to improve the performance of Software Vulnerability Prediction Models (VPMs) that currently predict if a piece of code is vulnerable or not (binary detection) but are limited to provide the specific type/family of vulnerability that needs to be further fixed and mitigated in the code. We present an automated multiclass vulnerability detection tool to improve the performance of Java VPMs. Our approach transforms the source code of vulnerable Java files into embeddings (n-dimensional numeric vectors) using code2vec, a deep-learning engine based on deep neural networks and attention mechanisms that decompose a program's code with Abstract Syntax Tree (AST) paths information as a versatile blend of syntax and semantics from a source code. We further take the numerical embedded representations of the vulnerabilities to train a Supervised Vector Machine (SVM) with a Radial Basis Kernel classifier to learn to detect the specific vulnerability family they belong to, according to the Common Weakness Enumeration (CWE) taxonomy. We evaluated our tool with open source, real-world Java repositories that provide ground truth labels for vulnerability instances across the repositories' history. Our results report classification metrics for two scenarios. First, an average F1-score of 97% (lowest of 95%, highest of 98%) when predicting vulnerable embeddings from CWE families with less training instances (900) but higher similarity across related CWE sub-families (e.g., CWE-79: cross-site scripting; CWE-89: SQL injection). Second, an average F1-score of 77%

2023 WiCyS CONFERENCE

STUDENT POSTERS

(lowest of 56%, highest of 88%) when predicting vulnerable embeddings from CWE families with higher number of training instances (2,000) and higher variance across related CWE sub-families (e.g. CWE-264: permissions, privileges and access controls; CWE-20/-22: improper input validation, path traversals; CWE-200: unauthorized exposure of sensitive information).

20. Improving Cybersecurity in Windmills: Toward Creating Green and Secure Technologies in Renewable Energy Systems

Brian G Rodiles Delgado; The University of Texas at El Paso, Nadia V Karichev and Christian Servin; El Paso Community College

In the last two decades, the world has witnessed the vulnerabilities of systems in cyberspace. Many people and companies have experienced hacks, data breaches and even ransomware attacks, which have left them exposed and in danger as their personal and classified information ends up in the wrong hands. However, the cybersecurity community has been actively working on ways to defend systems from threat actors. Still, there has been an enormous number of reported attacks on the industrial equipment of power plants, factories and electric grids, which many did not consider to be vulnerable to powerful and detrimental cyberattacks. With the ongoing transition from polluting ways to producing energy for renewable ones, wind farms are also part of those systems vulnerable in cyberspace. Moreover, ransomware has been the cause of many financial and informational losses as the energy industry has been the most targeted by threat actors between 2014 and 2021 (Dragos Inc., 2022). For those reasons, the intention of the project is to provide a methodology for analyzing ransomware attacks on wind farm scenarios. Even though operational technologies comprehend a vast number of systems and mechanisms, most of them share a Supervisory Control and Data Acquisition (SCADA) system. As there are many components targeted during a cyberattack in an operative technology system, an evaluation identified four paths to gain access to windmills: the SCADA Master Station LAN network, the wind turbine's network, the Wind Turbine Control Panel (WTCP), and the substation LAN network (Wu et al., 2019). However, we considered only the first two paths as attack vectors because the WTCP can only be manipulated physically, and the elements of the substation LAN network are part of the Energy Management System (EMS), which is protected through a cloud provider (Sun et al., 2018). By identifying the elements that play a role during a ransomware attack, we managed to create a simulation of a windmill and its network by using two Python programs for the Modbus protocol server and client, synthetic data to simulate windmills' sensor reading, and three virtual machines connected through an internal network that isolated them from the host machine and the outside world. In conclusion, the developed test bed provides a safe and controlled environment for testing ransomware in wind farm scenarios. Further work will determine the most efficient solutions against ransomware in any wind power facility.

21. User Behavior Helping Identify Security Threats in a Security Operations Center Environment

Kiranjit Kaur Shergill; Warwick University

The threat of cybercrime and the impact a cyberattack can have has lead organizations to develop security operations centers (SOC) to investigate and prevent threats to the network. Typically, a SOC will monitor network traffic and system logs to understand threats and identify potential attacks. The huge amounts of data generated have led to the development of security information event management (SIEM) systems. These systems reduce the workload for SOC operatives by automating some of the analysis and threat detection. Examining user behavior is one way to detect suspicious activity. If a user starts acting abnormal, then it might be an indication of an attack. However, user behavior has not been fully incorporated into SIEM systems to support SOC. This project explores how behaviors and machine learning is able to mitigate and detect security threats as there is currently no open-source solution for this problem. The project objectives are intended to be met by using a configured system for user profiling to simulate attacks on a device in order to assess if the system can successfully detect them or not. The methodology involves identifying Wazuh as a suitable open-source solution to monitor and log data in order to produce results for analysis. The results focused on user behavior related to insider threats, account compromise and data exfiltration. The findings produced were successful as the system positively generated the anticipated results but could use further improvement. The outcome of the thesis demonstrates that investigating user behavior can support SOC to identify unusual patterns and mitigate security threats.

22. STRIDE Security Modeling and Code Implementation

Anisha Srivastava; Simmons University

When designing software, developers spend most of their effort modeling functional requirements. Modeling non-functional requirements (NFRs), such as security and performance requirements, is not prioritized. We propose building on the UML modeling framework by providing a methodology to model NFRs in addition to functional requirements. Once NFRs are modeled, developers can clearly identify vulnerability points and insert code addressing these concerns, making the code more resilient to cybersecurity attacks. In the next phase of our research, this risk abatement code will be automatically injected upon parsing the class and sequence diagrams. In the following sections, we apply the STRIDE model to our motivating example and model the identified vulnerabilities in a class and sequence diagram. We focus on one specific abatement to clarify our approach.

2023 WiCyS CONFERENCE

STUDENT POSTERS

23. Misinformation on TikTok: Rampant Content, Lax Moderation and Vivid User Experiences

Jennifer Vander Loop, Filippo Sharevski and Amy Devine; DePaul University

This project reports an investigation of misinformation content on the TikTok platform and how real users experienced it through their daily interactions. Details about misinformation on TikTok are scarce and focus on misleading COVID-19 content. We sampled a population of 60 participants who were 18 and over, active TikTok account holders from the U.S. The qualitative responses were coded and categorized based on salient features that form a folk model, origins of misinformation, misinformation purpose, misinformation assessment, and tactical response to misinformation. Participants were asked to view four misinformation videos related to the topic of herbal at-home abortions and asked open-ended questions regarding their responses to the videos and the information on abortions being shared on TikTok. The paper will expand on how users conceptualize misinformation and develop resilience to the misinformation they encounter during social media use.

24. CNN Model for Classifying Audio Signals of IoT App Memory

Ramyapandian Vijayakanthan; Towson University, Irfan Ahmed; Virginia Commonwealth University and Aisha Ali-Gombe; Louisiana State University

As our cyberinfrastructure continues to advance, so does the sophistication of threats posed by bad actors. In particular, the IoT ecosystem has become a much easier and more accessible target for adversaries to execute the most evasive types of attacks, such as botnets. Often, these attacks occur due to the use of insecure network services or backend APIs, deprecated software components, unencrypted data communication, etc. Device memory fingerprinting and verification is one of the promising approaches for improving IoT security. The current state-of-the-art IoT security models leverage deep Convolution Neural Networks (CNN) for training and classifying known IoT malware. Although these models reported high accuracy, the major drawback is that they require a large sample of malware dataset for sufficient training of the proposed model; otherwise, the performance might degrade significantly. To overcome this drawback, we propose a novel framework of converting dynamic IoT device memory fingerprints into sound wave signals from which the Mel-Frequency Cepstral Coefficients (MFCC) and the Chroma features are extracted to train our CNN model for precise classification of the soundtracks. The transformation of memory into sound wave signals provides critical features in terms of frequency or pitch variations depending on the allocation of various memory components like the heap, code, stack, data, etc. These features contain distinctive properties that are effectively considered by our analysis engine to determine their similarities, differences or anomalies. We developed multiple IoT testbeds on Raspberry Pi 4 single-board computers (SBC) with various sensors to run different IoT applications. The runtime memory of each

testbed at different timestamps is acquired by a memory forensics acquisition tool called Memfetch. The acquired memory snapshots corresponding to each timestamp are converted into sound wave signals. There were a total of 20 IoT applications from which 10 sound wave signals were generated for each IoT application at different timestamps. In addition, we performed audio data augmentation using librosa's inverse polarity function to generate an augmented wave for each acquired wave. Our proposed framework preprocesses the transformed audio signals to extract their MFCC and condensed form of tonal features called Chroma features. The extracted features are passed to our CNN model, which contains two convolution layers with max pooling and three dense layers with dropouts. To train our model, 60 memory-audio signals, including the device acquired and the augmented waves from three different IoT applications, are leveraged. As a result, our model outperforms the existing models with a detection accuracy of 100% without the need for extensive training datasets. This promising result can be applied to developing a sound intrusion detection model.

25. MiSSCyM: A Manufacturing Simulation Framework for Cyber Experimentation

Bethanie Williams; Tennessee Technological University

A revolution in manufacturing systems is underway as smart manufacturing has become a key component of the broader push toward Industry 4.0. Smart manufacturing is often considered the next generation manufacturing model that integrates advanced Information and Communication Technologies (ICT) to further improve the overall process, efficiency and profits in manufacturing systems. While the manufacturing industry is constantly evolving and increasing its sophistication, the need for simulation systems and testbeds is a top priority for researchers and manufacturing organizations. The development of manufacturing simulation systems plays an integral role in the advancement of manufacturing processes and operations because of its ability to replicate production-based concepts. Through the utilization of simulation systems, researchers and organizations are attempting to make manufacturing systems more secure by testing novel ideas before they are applied on working systems. This results in lowering costs and human risk while improving efficiency and production processes. Many manufacturing organizations use standardized communication protocols so that machines can effectively communicate with each other. Currently, the MTConnect standard is one of the most used communication protocols in the industry, as it allows machines and software applications to exchange data in an effective manner. This poster focuses on the development of a MTConnect-based simulator that can replicate data produced by actual machines at manufacturing facilities. The proposed simulation system - called MTConnect integrated Simulation System for Cyber Manufacturing (MiSSCyM) - can replay MTConnect data to analyze how machines are connecting, communicating or moving various parts. Most importantly, security tests can be applied to the simulation framework aimed specifically at manufacturing systems to gain a better understanding and insight into how security challenges impact machines' performances, communications and other actions.

2023 WiCyS CONFERENCE

STUDENT POSTERS

26. Attack and Fault Detection in Internet of Things Using Graph Neural Networks

Rozhin Yasaei; University of California Irvine

In today's world, we are surrounded by interconnected networks of intelligent devices called the Internet of Things (IoT) that monitor and control our home environment, workplace, health, vital infrastructure, factory planes, etc. The widespread presence of IoT systems and their critical applications emphasize the importance of their security and integrity. IoT devices are vulnerable to attacks and failures due to low computational resources, cost constraints and tight time-to-market. It is challenging to mitigate these attacks and failures because of the multidisciplinary nature of IoT, which brings together the physical domain through sensor interaction and the cyber domain through the communication network and cloud. Although numerous stand-alone approaches are proposed in the literature for network intrusion detection or sensor anomaly detection, a holistic model is missing to integrate the information from both domains and extract the valuable context shared among different system components. To address these, we present a novel approach for multi-modal data fusion that fuses sensor and communication data for the first time. We integrate IoT physical and cyber elements into a graph representation that signifies the correlation between elements as a connection and provides embedding for data generated by each component. We construct a graph neural network (GNN) model to learn the context and normal state of the system and detect abnormal activities. We further study the signatures of networks and sensor attacks to determine the source of the anomaly to facilitate fast and informed recovery after an incident. Our model is optimized to be executed on a fog-based platform for real-time system supervision. Our experiment on greenhouse monitoring IoT systems demonstrates that our approach, on average, achieves 22% F1-score improvement over the single-modal techniques for anomaly detection.

27. 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.

28. Accelerating In-Vehicle Network Intrusion Detection System Using Binarized Neural Network

Linxi Zhang, Di Ma; University of Michigan-Dearborn and Xuke Yan; Oakland University

Controller Area Network (CAN), the de facto standard for in-vehicle networks, has insufficient security features and thus is inherently vulnerable to various attacks. To protect CAN bus from attacks, intrusion detection systems (IDS) based on advanced deep-learning methods, such as Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN), have been proposed to detect intrusions. However, those models generally introduce high latency, require considerable memory space, and often result in high-energy consumption. To accelerate intrusion detection and also reduce memory requests, we exploit the use of Binarized Neural Network (BNN) and hardware-based acceleration for intrusion detection in in-vehicle networks. As BNN uses binary values for activations and weights rather than full precision values, it usually results in faster computation, smaller memory cost and lower energy consumption than full precision models. Unlike other deep-learning methods, BNN can be further accelerated by leveraging Field-Programmable Grid Arrays (FPGA) since it cuts down the hardware consumption. We designed our BNN model to suit CAN traffic data and exploit sequential features of the CAN traffic instead of individual messages. We evaluated the proposed IDS with four different real vehicle datasets. Our experimental results show that the proposed BNN-based IDS reduces the detection latency on the same CPU (three times faster) while maintaining acceptable detection rates compared to full precision models. We also implemented the proposed IDS using FPGA hardware to reduce latency further and accelerate intrusion detection. Our experiments on multiple platforms demonstrated that using the FPGAs dramatically reduces the detection latency (128 times faster) with lower power consumption in comparison with an embedded CPU.

Be a part of the network life.

Join the Verizon Cybersecurity team.

Here, you can power up your career with a wide range of opportunities in this diverse field. And with access to the latest tools and technologies, you can make a positive impact every day as you continue to build your skills and your future. From Security Operations, Risk Management, Engineering and beyond, discover a future without limits.

Explore roles at:
verizon.com/cybersecurity

verizon✓

Heather W.
Cybersecurity—Program and
Project Management Consultant



securing.information
for the
future of retail;



Ready to join a team of cybersecurity experts who make an epic impact and are at the forefront of the next retail disruption?

Explore all of the opportunities our
InfoSec team has to offer.

Walmart * Global Tech
tech.walmart.com

2023 WiCyS CONFERENCE

SPEAKER INDEX

KEYNOTE SPEAKERS			
NAME	AFFILIATION	TWITTER HANDLE	DATE AND TIME
Erin Heinmiller	Raytheon		Friday Dinner Keynote
Barbara Kosloski	Optum		Friday Lunch Keynote
Sylvia Schlaphof	Fortinet		Friday AM Keynote
FEATURED SPEAKERS			
NAME	AFFILIATION	TWITTER HANDLE	DATE AND TIME
Korrey Anderson	SentinelOne		Friday Lunch Keynote
Katie Boudreau	Mastercard		Friday Dinner Keynote
Aditi Chaudhry	Two Sigma		Saturday AM Keynote
Deborah Golden	Deloitte		Friday AM Keynote
Sharnikya Howard	Amazon		Friday Dinner Keynote
Pam Lindemoen	Cisco	@pamlindemoen	Friday Dinner Keynote
Molly Moore	NSA	@MollyMd913	Friday Lunch Keynote
Rebecca Moore	Shopify		Saturday AM Keynote
Archana Ramamoorthy	Google		Friday Lunch Keynote
Aj'a Dehavalland Taylor	Palo ALto		Saturday AM Keynote
Amy Tidwell	DeVry		Saturday Lunch Keynote
Heather Vermillion	PACCAR	@storyteller_hv	Saturday AM Keynote
Kemba Walden	Office of the National Cyber Director		Friday AM Keynote
Blakely Wall	Verizon		Friday AM Keynote
Melissa Yandell	Walmart	@mel03821575	Friday AM Keynote
PROGRAM SPEAKERS			
NAME	AFFILIATION	TWITTER HANDLE	DATE AND TIME
Morgan Adamski	National Security Agency	@adamski_morgan	Thursday, 5:35pm - 6:30pm
Jummy Adejuyigbe	Goldman Sachs		Saturday, Noon - 12:45pm
Dalal Alharthi	University of Arizona	@DalalHarthi	Saturday, 2:30pm - 4:30pm
Carly Battaile	Aon		Friday, 1:55pm - 2:40pm
Shiri Bendelac	The MITRE Corporation		Friday, 11:00am - 11:45am
Ashley Billman	Pacific Northwest National Laboratory		Thursday, 2:00pm - 4:00pm
Priyam Biswas	Intel	@amipri	Saturday, 2:30pm - 4:30pm
Debby Briggs	NetScout	@DebBriggs	Saturday, 11:00am - 11:45am
Eric Brown	CEROC / Tennessee Tech University	@elbrownmcne	Saturday, 2:30pm - 4:30pm
Cheri Caddy	Office of the National Cyber Director/ The White House		Saturday, 10:00am - 10:45am
Jazmin Coronado	Viasat		Friday, 11:00am - 11:45am and Friday, 4:45pm - 5:30pm
Caitlin Delmore	Palo Alto Networks		Saturday, 11:00am - 11:45am
Mary Diner	UnitedHealth Group		Friday, 4:45pm - 5:30pm
Diane Downie	Synopsys		Thursday, 2:00pm - 4:00pm
Denise Dragos	St. John's University, Queens, New York	@Dubbd	Saturday, 2:30pm - 4:30pm
Jeremy J. Epstein	NSF		Thursday, 7:00pm - 8:30pm
Maya Flores	Amazon Web Services		Thursday, 4:30pm - 6:30pm
Glorianne Francavilla	Viasat		Friday, 4:45pm - 5:30pm

2023 WiCyS CONFERENCE

SPEAKER INDEX

PROGRAM SPEAKERS			
NAME	AFFILIATION	TWITTER HANDLE	DATE AND TIME
Kozeta Garrett	Microsoft		Saturday, noon - 12:45pm
Lauren Goldman	Office of the Director of National Intelligence		Thursday, 5:35pm - 6:30pm
Esther Goldstein	Salesforce		Thursday, 12:30pm-1:30pm
Silka Gonzalez	ERM Protect		Saturday, noon - 12:45pm
Ashley Greeley	National Cryptologic University, NSA		Thursday, 4:30pm - 5:25pm and Thursday, 7:00pm - 8:30pm
Emily Hacker	Microsoft	@dreadphones	Saturday, 2:30pm - 4:30pm
Courtney Hans	CareRev	@WkndAdventur	Friday, 2:50pm - 4:40pm
Elaine Harrison-Neukirch	Scythe	@rubysgeekymom	Friday, 4:45pm - 5:30pm
Elizabeth K. Hawthorne	Rider University		Thursday, 12:30pm-1:30pm
Kelsey Helms	Target		Saturday, noon - 12:45pm
Allison Henry	University of California, Berkeley		Saturday, 10:00am - 10:45am
Hanan Hibshi	Carnegie Mellon University	@HananHibshi	Saturday, 11:00am - 11:45am
Ann-Marie Horcher	Northwood University	@doktorrie	Saturday, 11:00am - 11:45am
Meghan Jacquot	Inspectiv	@CarpeDiemT3ch	Thursday, 4:30pm - 6:30pm
Angie Jin	Fortinet		Saturday, 10:00am - 10:45am
Erin Joe	Mandiant, a Google Cloud Company		Friday, 1:55pm - 2:40pm
Kyle Jones	Sinclair College		Thursday, 4:30pm - 6:30pm
Apoorva Joshi	Elastic	@joshaaayyyyy	Saturday, 10:00am - 10:45am
Cynthia Kaiser	Federal Bureau of Investigation		Saturday, noon - 12:45pm
Simeon Kakpovi	Microsoft	@simandsec	Saturday, 2:30pm - 4:30pm
Angie Kalaytowitz	UnitedHealth Group		Friday, 4:45pm - 5:30pm
Deborah Kariuki	University of Maryland Baltimore County		Saturday, 11:00am - 11:45am
Alisha Kloc	Security Consultant		Saturday, 10:00am - 10:45am
Arica Kulm	Dakota State University		Saturday, noon - 12:45pm
Chyna Lane	University of the Incarnate Word and Southwest Research Institute		Thursday, 12:30pm-1:30pm
April Lenhard	Team Cymru		Saturday, noon - 12:45pm
Litany Hope Lineberry	Mississippi State Univ.		Thursday, 12:30pm-1:30pm
Laura Malave	St. Petersburg College	@lauramalave	Friday, 4:45pm - 5:30pm
Julie Marquez	Palo Alto Networks		Saturday, 11:00am - 11:45am
Amanda Martens	The Department of Homeland Security		Friday, 1:55pm - 2:40pm
Sofia Martinez	Northern Trust		Friday, 2:50pm - 4:40pm
Camila Martins	Microsoft	@camomila_mila	Saturday, 10:00am - 10:45am
Adrienne McCloud	Aerospace Village		Saturday, noon - 12:45pm
Lauren McGlinch	Federal Bureau of Investigation		Saturday, noon - 12:45pm
Aleise McGowan	WiCyS Neurodiversity Affiliate		Thursday, 12:30pm-1:30pm
Megan McIntyre	Synopsis		Thursday, 2:00pm - 4:00pm
Vickie McLain	Alexandria Technical and Community College		Saturday, 2:30pm - 4:30pm
Teresa Merklin	Lockheed Martin		Saturday, noon - 12:45pm
Alexis Merritt	Cisco Systems	@ReckedExe	Thursday, 2:00pm - 4:00pm
Leigh Metcalf	CERT	@theladyofgeek	Saturday, 10:00am - 10:45am

2023 WiCyS CONFERENCE

SPEAKER INDEX

PROGRAM SPEAKERS			
NAME	AFFILIATION	TWITTER HANDLE	DATE AND TIME
Alyssa Miller	Epiq Global	@alyssam_infosec	Friday, 11:00am - 11:45am and Friday, 2:50pm - 4:40pm
Erin Miller	Space ISAC		Saturday, noon - 12:45pm
Tauna Mills	Argoz Advisory LLC		Thursday, 2:00pm - 4:00pm
Jennifer Miosi	Aircraft Cybersecurity and United Express Partners Cybersecurity; United Airlines		Saturday, noon - 12:45pm
Kirsten Mitchell	Palo Alto Networks		Saturday, 11:00am - 11:45am
Jennifer Munoz	Northern Trust		Friday, 2:50pm - 4:40pm
Sunny Myers	Palo Alto Networks		Saturday, 11:00am - 11:45am
Danny Navo	Amazon Web Services		Thursday, 4:30pm - 6:30pm
Perri Nejib	Northrop Grumman		Saturday, 10:00am - 10:45am
Suzanne Nielsen	Office of the National Cyber Director		Friday, 11:00am - 11:45am and Friday, 2:50pm - 4:40pm
Noureen Njoroge	WiCyS North Carolina		Friday, 2:50pm - 4:40pm
Sasha Cohen O'Connell	American University		Saturday, 10:00am - 10:45am
Collins Okafor	WiCyS University of Houston Student Chapter		Thursday, 12:30pm-1:30pm
Staci Hill Okine	Palo Alto Networks	@staciokine	Saturday, 11:00am - 11:45am
Tolu Onireti	Oracle		Saturday, noon - 12:45pm
Alison Owens	University of South Florida		Saturday, 11:00am-11:45am
Albert Palacios	DoEd		Thursday, 4:30pm - 5:25pm
Radha Parikh	EY		Friday, 1:55pm - 2:40pm
Quintana Patterson	University of Colorado School of Medicine Anschutz Medical Campus		Friday, 2:50pm - 4:40pm
Elena Peterson	Pacific Northwest National Laboratory		Thursday, 2:00pm - 4:00pm
Kassandra Pierre	WiCyS Neurodiversity Affiliate		Thursday, 12:30pm-1:30pm
Ashley Podhradsky	Dakota State University	@AshleyPodhrads1	Saturday, noon - 12:45pm
Ruchira Pokhriyal	Amazon Web Services	@Silver_Banshee1	Saturday, 10:00am - 10:45am
Davina Pruitt-Mentle	NICE/NIST/DOC		Thursday, 4:30pm - 5:25pm
Taylor Pyle	Viasat		Friday, 11:00am - 11:45am
Michael Qaissaunee	Brookdale Community College		Thursday, 4:30pm - 6:30pm
Elizabeth Rasnick	Center for Cybersecurity at the University of West Florida		Thursday, 12:30pm-1:30pm
Veena Ravishankar	University of Mary Washington		Friday, 2:50pm - 4:40pm
Lisa Raykowski	EY		Saturday, 10:00am - 10:45am
Jessica Robinson	WiCyS	@JessRobin96	Thursday, 4:30pm - 6:30pm and Friday, 2:50pm - 4:40pm
Harley Rohrbacher	LookingGlass Cyber Solutions		Saturday, noon - 12:45pm
Dianne Rose	Asurion		Thursday, 12:30pm-1:30pm
Kendra Russell	South Dakota Division of Criminal Investigation		Saturday, noon - 12:45pm
Gatha Sathir	Carnival Corporation		Saturday, noon - 12:45pm
Smruthi Sandhanam	Northrop Grumman		Saturday, 10:00am - 10:45am
Fatoumata Sankare	Datacation LLC		Friday, 4:45pm - 5:30pm
Suzanna Schmeelk	St. John's University, Queens, New York		Saturday, 2:30pm - 4:30pm
Olivia Schmidt	University of South Florida		Saturday, 11:00am-11:45am

2023 WiCyS CONFERENCE

SPEAKER INDEX

PROGRAM SPEAKERS			
NAME	AFFILIATION	TWITTER HANDLE	DATE AND TIME
Saskia Laura Schroeer	Cisco Systems		Thursday, 4:30pm - 6:30pm
Steph Shample	Middle East Institute	@snshamp	Saturday, noon - 12:45pm
Katie Shuck	South Dakota Fusion Center	@katieshuck	Saturday, noon - 12:45pm
Justin Simpson	Walmart Global Tech		Saturday, 11:00am - 11:45am
Kavitha Sivagnanam	Palo Alto Networks		Saturday, 11:00am - 11:45am
Alice E. Smitley	National Centers of Academic Excellence in Cybersecurity		Thursday, 7:00pm - 8:30pm
Molly Soja	Bank of America		Saturday, 10:00am - 10:45am
Diane Stephens	University of Georgia		Saturday, 11:00am - 11:45am
Camille Stewart Gloster	Office of the National Cyber Director	@CamilleSG46 and @CamilleEsq	Friday, 11:00am - 11:45am and Friday, 2:50pm - 4:40pm
Aishwarya Surani	University of Denver		Saturday, 11:00am - 11:45am
Cynthia Sutherland	Amazon Web Services		Thursday, 2:00pm - 4:00pm
Holly Syed	Arctic Wolf		Thursday, 2:00pm - 4:00pm
Paul Tortora	United States Naval Academy		Friday, 2:50pm - 4:40pm
Jolie Grace Wareham	Tennessee Democratic Party Cyber Safety Committee; Vanderbilt Uni.	@jgfortennessee	Saturday, 11:00am - 11:45am
Samara Williams	New Relic	@SamaraaaRW	Thursday, 4:30pm - 6:30pm
Abby Willis	Walmart		Saturday, 11:00am - 11:45am
Lily Yeoh	CIRisk		Thursday, 2:00pm - 4:00pm
CAREER VILLAGE TALK SPEAKERS			
NAME	AFFILIATION	TWITTER HANDLE	DATE AND TIME
Dawn Beyer	Lockheed Martin		Thursday, 2:00 pm - 2:30pm
Julia Costin	University of Colorado (Colorado Springs)		Friday, 9:45am - 10:15am
Veronica Doak	Google		Thursday, 2:30 pm - 3:00pm
Lynn Dohm	WiCyS		Thursday, 2:30 pm - 3:00pm
Tonia Dudley	COFENSE		Thursday, 3:00pm - 3:30pm
Fatemeh Ebrahimi	Optum		Thursday, 4:00pm - 4:30pm
Nakia Grayson	NIST		Thursday, 2:30 pm - 3:00pm
Rachael Klamo	Optum		Thursday, 4:00pm - 4:30pm
Toby Liftee	Palo Alto Networks		Friday, 10:15am - 10:45am
Ashley Mahoney	University of Alabama in Huntsville		Thursday, 4:30pm - 5:00pm
Lisa McKee	Dakota State University		Thursday, 2:30 pm - 3:00pm and Thursday, 3:30pm - 4:00pm
Marti Mondragon	Palo Alto Networks		Friday, 10:15am - 10:45am
Ossie Munroe	Bloomberg		Friday, 11:15am - 11:45am
Perri Nejib	Northrup Grumman		Thursday, 2:00 pm - 2:30pm
Bryn Preuss	Palo Alto Networks		Friday, 10:15am - 10:45am
Smruthi Sandhanam	Northrup Grumman		Thursday, 2:00 pm - 2:30pm
Lauren Strobe	Adobe		Friday, 10:45am - 11:15am



Learn how we help you build more trusted user experiences

Subscribe to our newsletter.

www.adobe.com/go/securitynews



Take your career to new heights with American Airlines.

Apply today at jobs.aa.com



American Airlines 

AON

We Believe Businesses Thrive When People Flourish

Aon is proud to support WiCyS and their dedication to promoting diversity and the success of women in cyber security.

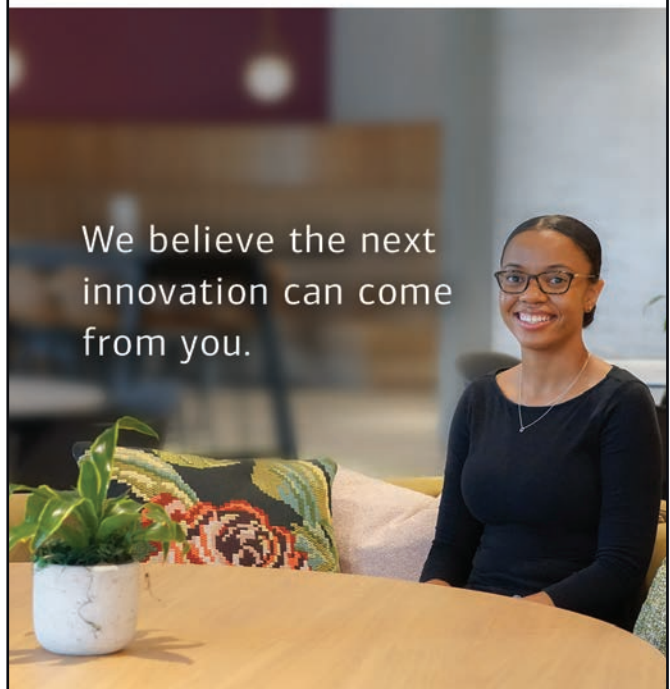
Learn more:
aon.com/cyber-resilience



BANK OF AMERICA



We believe the next innovation can come from you.



BBH is proud to support Women in Cyber Security

Visit bbh.com/careers
to explore opportunities.

 BROWN BROTHERS HARRIMAN



We're Hiring! Come Join Our Team

Check Point was recognized by
Forbes as a 2022 Best Employer!
Come join us. It's a great place to be.

See what openings we have here:



*Come join our team and experience
the world of cybersecurity in its
complete spectrum and diversity!*

CEROC Info



CS Graduate Info



The Cybersecurity Education, Research and Outreach Center at Tennessee Tech University seeks the enrichment of the cybersecurity community and its members through education program development, effective research into emerging areas of need, and outreach to students of all ages and grade levels encouraging their participation in STEM experiences and the excitement of the cybersecurity field.

- NCAE-C Center of Academic Excellence – Cyber Defense
- First and Largest CyberCorps SFS program in the State of TN
- Only DoD Cyber Scholarship (CySP) program in TN
- CyberEagles and WiCyS student cybersecurity clubs
- WiCyS Conference – Founding Institution and First Student Chapter
- GenCyber Camp and GenCyber on Wheels Programs
- Cyber Interest Groups in CTF, Defense, and Offensive Security



CSSIA
National Support Center for Systems
Security and Information Assurance



The Center for Systems Security and Information Assurance (CSSIA) has instructed more than 2000 teachers and college faculty in cybersecurity related areas. CSSIA strives to bring the best and most current courses to you throughout the year and works with the National Science Foundation (NSF) Advanced Technology Education (ATE) grant programs and industry partners to define and organize these efforts. Visit our website to view our courses now!

CSSIA.org

ECS

JOIN US

IN BUILDING A
BETTER CYBER TEAM

We're currently hiring analysts,
engineers, and more.



Apply Today!



JOIN OUR ELITE CYBERSECURITY TEAM



THE FBI IS HIRING SPECIAL AGENTS, COMPUTER SCIENTISTS AND DATA ANALYSTS

BOOTH 132 **FBIJOBS.GOV**

Congratulations to Women in Cybersecurity (WiCyS) on your 10th Annual Conference.



Huntington
Welcome.®

Member FDIC. © 2023 Huntington Bancshares Incorporated.



MADISON

Executive VP of Security
& Operations



KELLY

Blue Team Service Manager



NIAMBI

Office Administrator



JORI

Blue Team Coordinator

We are the faces of Cybersecurity We are JSCM Group

Visit Booth 312 to learn about our career opportunities.
www.jscmgroup.com/careers-wicys



JSCM GROUP
CYBERSECURITY TESTING, TRAINING & MANAGEMENT



APPLY TODAY

Only here can I find my
purpose at home and work.

LOCKHEED MARTIN



Priyanka
Systems Engineer



MorganFranklin Consulting Cybersecurity Services

Assisting clients
across the globe to
solve their most
complex cybersecurity
challenges.



OUR END-TO-END OPPORTUNITIES

- Strategy & Risk
- Identity & Access Management (IAM)
- Security Operations (SecOps)
- Cyber & Operational Resilience (CORe)
- Digital Forensics & Incident Response (DFIR)
- Managed Security Services Provider (MSSP)



To learn what
it means to
own your career,
visit us at

morganfranklin.com/careers



Let's transform
together

Protiviti is here to help influence the technology industry and empower Protiviti's women to become leaders in the workplace. **Let's transform together.**

protiviti
Global Business Consulting

protiviti.com



RICE UNIVERSITY
Department of Computer Science

“Women can contribute tremendous diversity of thought towards cybersecurity solutions. The way forward is inclusion so more women know that cybersecurity is where they belong.”



Dr. Janell Straach, Ph.D
Chair of the Board, WiCyS
Lecturer, Rice Computer Science

See how Janell advances cybersecurity education






Exceptional People. Exceptional Contributions.

Cyber threats have accelerated due to our increased reliance on the always-connected, digital landscape. Infrastructure failures and ransomware are just a couple examples of threats Sandia addresses. The need to understand interdependencies, increase national infrastructure resilience, and mitigate cyber risks is essential.

Come join us in implementing innovative technologies to anticipate and thwart cyber threats today and into the future.

For an exceptional career, visit sandia.gov/careers

All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, age, disability, or veteran status and any other protected class under state or federal law.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525. SAND2023-12626M



Land a career with Heart.

At Southwest®, you're empowered to create your own career; one that fits the goals-and lifestyle-you want. Get a career by you, for you.



Connect with us at:
swa.is/HiringOutreach

Southwest®



we're hiring
careers.tiktok.com

TikTok's Global Security Organization provides a comprehensive suite of shared services to protect our most critical assets by securing our people, processes, and technology. If you're looking for your next challenge, we'd love to hear from you!

CYBERSECURITY SERVICE U.S. DEPARTMENT OF HOMELAND SECURITY

OUR NATION'S CYBERSECURITY AND YOU.

We need women like you to help protect the systems, networks, and information Americans rely on. **Join the DHS Cybersecurity Service** and design the career path that builds on your interests and unique talents.

Come visit us at booth #213!

LEARN MORE AND APPLY
DHCS.USAJOBS.GOV





**We support
women in
cybersecurity.**

**Come connect with the team
that is building the largest
platform for all things home!**



**A workplace that
works for women.**

At Workday, we believe opportunity should be for everyone.

That's why we're cultivating a workplace that welcomes diverse perspectives and empowers women to succeed in whatever role they choose.

Come join a company where women are valued and where women lead: workday.com/careers

©2023 Workday, Inc. All rights reserved.
Workday and the Workday logo are registered
trademarks of Workday, Inc. All other brand and
product names are trademarks or registered
trademarks of their respective holders.



Build your edge. Build what's next.

Join a community of changemakers, innovators, and doers. Join Zebra.

We're Hiring!

View Zebra Technologies openings at www.zebra.com/careers

VISIT THE CAREER FAIR

ORGANIZATION	BOOTH #
Accenture	116
Activision	No Booth
Adobe	308
Amazon Web Services	300/302
American Airlines	411
American Express	119
Antisyphon Training (Black Hills Information Security)	226
AON	238
Arctic Wolf	227
Aristocrat	326
Asurion	214
Bank of America	112
Battelle	327
Bloomberg L.P.	101/103
BrainGu	426
Brown Brother Harriman	438
Capitol Technology University	427
Carnegie Mellon University INI	128
Carnegie Mellon University Software Engineering Institute	206/208
CGI Group	236
Champlain College	129
Check Point Software Technologies	204
Cisco System Security & Trust Organization	113/115
CME Group	228
Comerica	237
CrowdStrike	216
Cyberbit	229
CybHER at DSU	218
Defense Intelligence Agency	317
Dell Technologies	319
Deloitte	314/316
DeVry University	215/217
DHS Cybersecurity Service	213
Drexel University College of Computing & Informatics	328
ECS Federal	405
Envestnet Inc.	412
EY	414
Federal Bureau of Investigation (FBI)	132
Florida International University	418
Fortinet	100/102
GE Gas Power	437/439

ORGANIZATION	BOOTH #
Georgia Tech Research Institute	413
Goldman Sachs	310
Google	406/408
Grainger	415
Huntington National Bank	409
IBM	120
Idaho National Laboratory	417
ISC2 - International Information System Security Certification Consortium, Inc.	428
Johns Hopkins School Advanced International Studies	421
JPMorgan Chase & Co.	429
JSCM Group	312
LinkedIn	No Booth
Lockheed Martin	400
ManTech	123
Marqeta	124
Marshall University College of Engineering and Computer Sciences	133
Mastercard	105/107
Metropolitan State Univ of Denver	436
MIT Lincoln Laboratory	232
MorganFranklin Consulting, Cybersecurity	125
Motorola Solutions	338
National Center for Systems Security and Information Assurance (CSSIA)	313
National Security Agency	402/404
Naval Information Warfare Center, Pacific	222
NCyTE Center @ Whatcom Community College	315
Nestle Purina	223
NETSCOUT	No Booth
New York Independent System Operator	233
New York University - Tandon School of Engineering	332
NICE - Nat'l Initiative for Cybersecurity Education	333
North Carolina Partnership for Cybersecurity Excellence	224
Northeastern University Khoury College of Computer Sciences	225
NuHarbor Security	432
Optum	201/203
PACCAR	209/211
Palo Alto Networks	305/307
Paychex	433
Protiviti	304
Purdue University	138 (POD)

VISIT THE CAREER FAIR

ORGANIZATION	BOOTH #
Raytheon Technologies	401/403
Regis University	137 (POD)
Rider University	137 (POD)
Rochester Institute of Technology (RIT)	322
Sandia National Laboratories	104
SANS Institute	323
Secure World	138 (POD)
Security Risk Advisors	324
SentinelOne	301/303
ServiceNow	114
Shopify	200/202
Southwest Airlines	416
Spectrum	325
SpecterOps	No Booth
Starbucks	134
SWIFT	422
Target	423
Tennessee Tech University - CEROC	212
The Home Depot	329
TikTok	239
Trend Micro Inc.	424
Truffle Security Co.	135
U.S. Army Corps of Engineers	336
U.S. Department of State	234
UCLA Health	235
University College University of Denver	139 (POD)
University of Colorado - Colorado Springs	425
University of South Alabama	139 (POD)
University of Washington Bothell	334
University of Washington, Tacoma	335
Vectra AI	126
Verizon /Basis Technologies	337/339
Victoria's Secret & Co	127
Visa Inc.	434
Walmart	108/110
Wayfair	309
Wentworth Institute of Technolog	435
Workday	205
Yubico Inc.	136
Zebra Technologies	109

WICYS COMMUNITIES

PROFESSIONAL AFFILIATE COMMUNITY

No matter who, or where you are, WiCyS provides you with the resources to connect, mentor, learn from and encourage other members. Interested in forming a new WiCyS Affiliate or associating with an existing one?

Scan the code below to learn more about WiCyS Professional Affiliates.



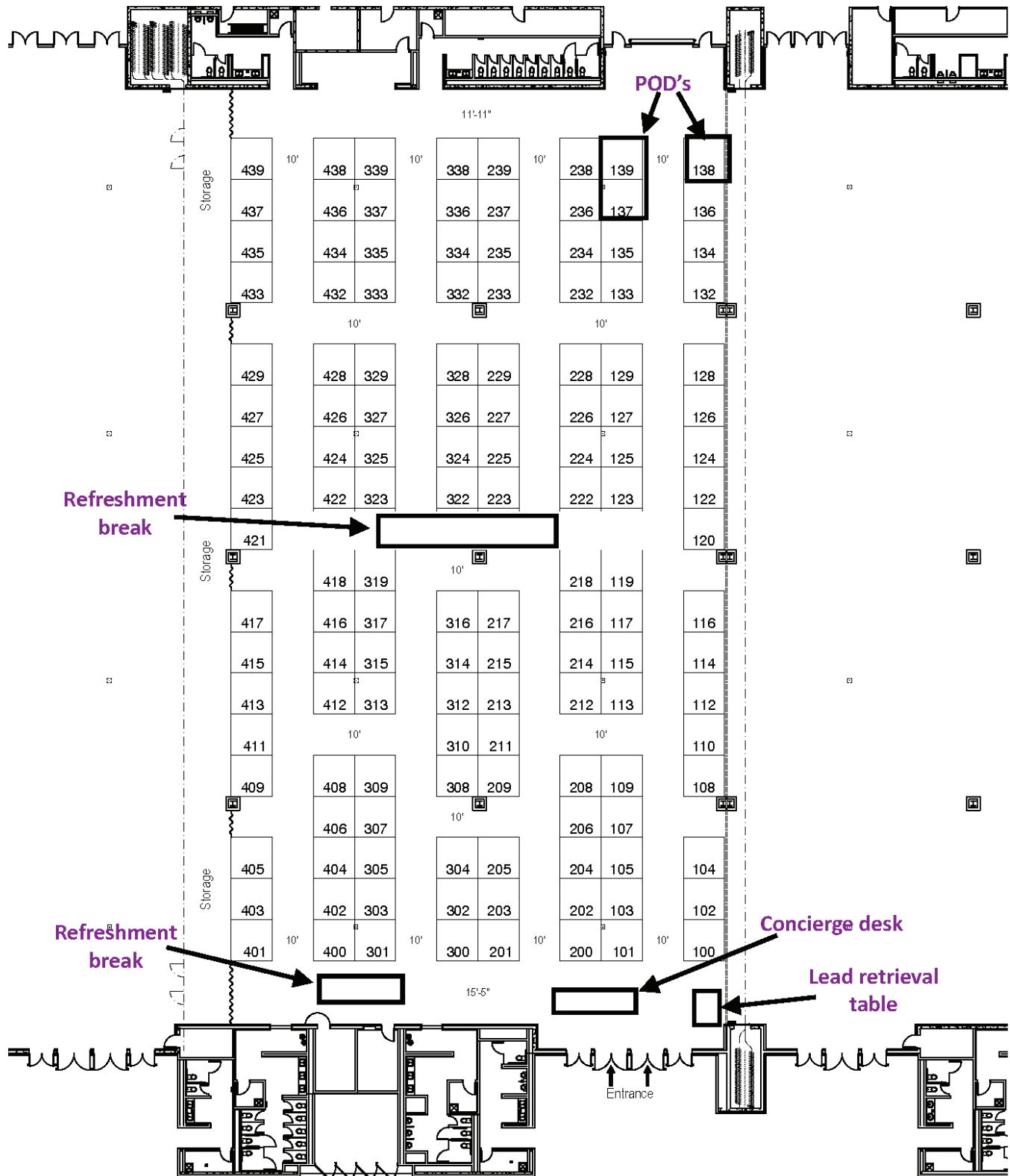
STUDENT CHAPTER COMMUNITY

WiCyS Student Chapter members gain access to industry and academic leaders who are eager to help them succeed. Student Chapter leaders also receive prioritized opportunities for WiCyS initiatives. Come together with your school's community of students in cybersecurity and start a WiCyS Student Chapter or join an existing one!

Scan the code below to find details on how to start a student chapter or to view a list of current chapters.



VISIT THE CAREER FAIR

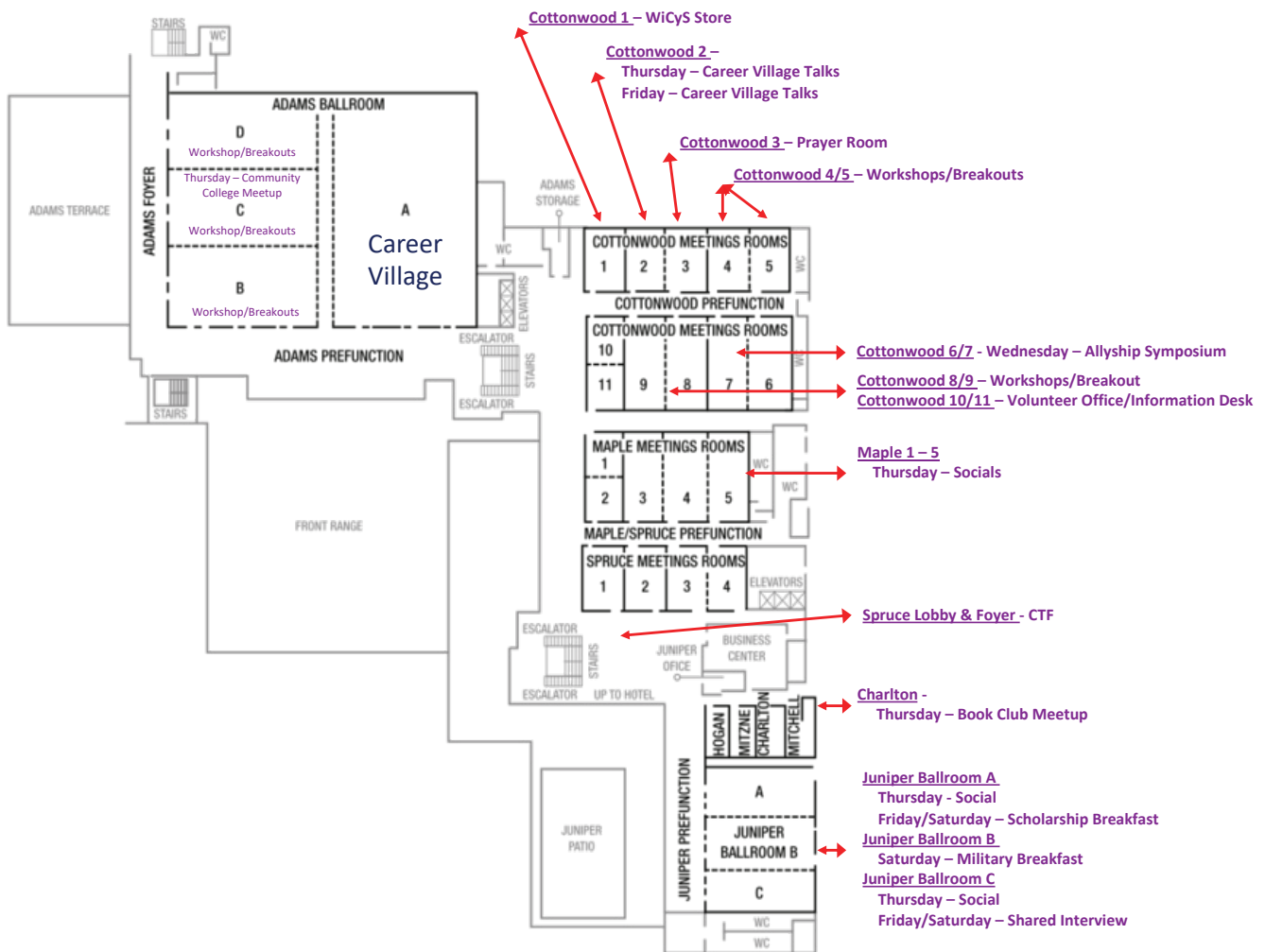


EVENTS, PRIZES, TRAVEL AWARDS & SPECIAL ITEMS

THANK YOU SPONSORS

ORGANIZATION	ITEM(S)
Adobe	Career Village Funding and Scholarship with Travel
Amazon	Mid-Career Breakfast and Scholarships with Travel
AWS Philanthropies	Scholarships with Travel
Bloomberg L.P.	Military Breakfast, Career Village Funding Sponsor and Scholarships with Travel
Booz Allen	Scholarships with Travel
CheckPoint	Scholarship with Travel
Cisco System Security & Trust Organization	Conference Bag and Scholarships with Travel
Carnegie Mellon University Software Engineering Institute	Selfie Station
Deloitte	Scholarships with Travel
Devry	Scholarship with Travel
Envestnet Inc.	Scholarships with Travel
Fortinet	Charging Station and Scholarships with Travel
GE Gas Power	Scholarships with Travel
Goldman Sachs	Scholarships with Travel
Google	Scholarships with Travel
Intel	Scholarship with Travel
LinkedIn	Scholarship with Travel
Lockheed Martin	Military Breakfast
Mastercard	Scholarships with Travel
Meta	Scholarship with Travel
Microsoft Philanthropies	Scholarships with Travel
MorganFranklin Consulting, Cybersecurity	Scholarship
NCyTE Center @ Whatcom Community College	Scholarships with Travel
Nestlé Purina	Scholarship with Travel
NetScout	Scholarships with Travel
Optum	Friday Lunch and Military Breakfast
PACCAR	Scholarships with Travel
Palo Alto Networks	Scholarships with Travel
Phylum	Scholarship with Travel
Raytheon	Scholarships with Travel
SentinelOne	Lanyard and Scholarships with Travel
Shopify	Scholarships with Travel
SpecterOps	Scholarships with Travel
Target	Selfie Station
Tennessee Tech University: DoD Cybersecurity Capacity Grant	Scholarships with Travel
Verizon / Basis Technologies	Mid-Career Breakfast and Scholarships with Travel
Walmart	Scholarships with Travel

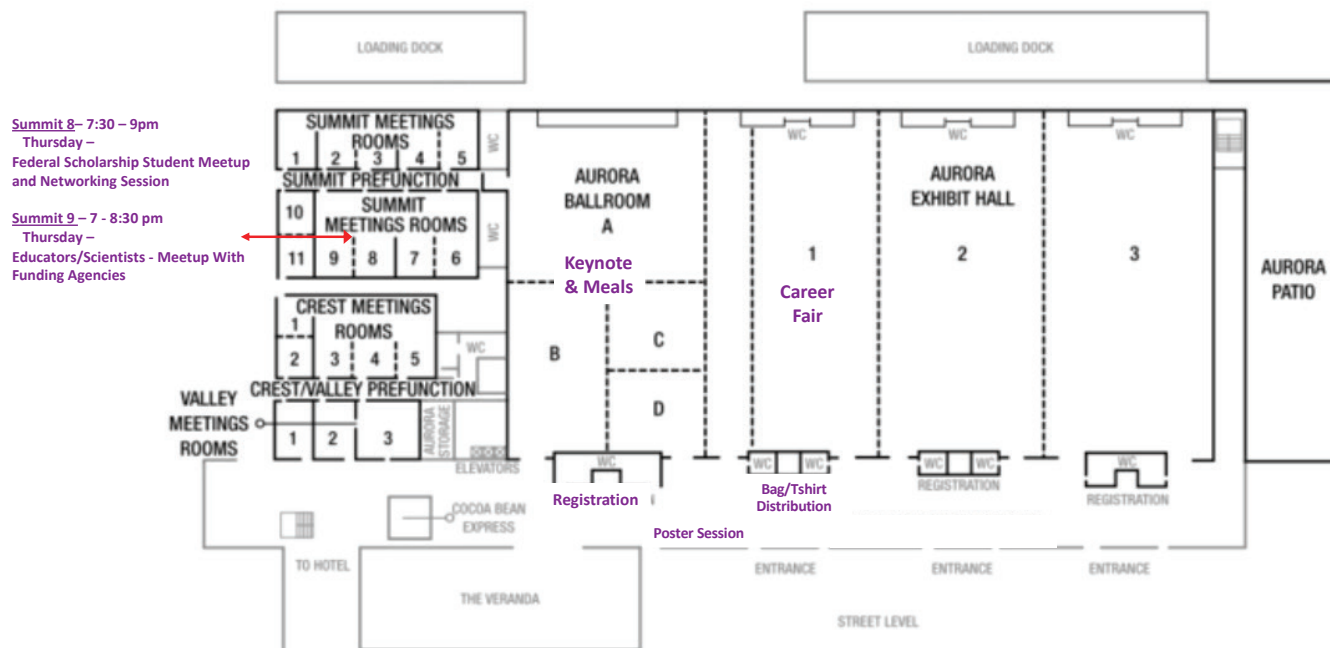
GAYLORD CONVENTION CENTER LEVEL 1



2023 WiCyS CONFERENCE

VENUE MAPS

GAYLORD CONVENTION CENTER LEVEL 2



women in
CYBERSECURITY

WiCyS



#SeeHerAsEqual



JOIN WiCyS IN SUPPORTING WOMEN IN CYBERSECURITY

Join Women in CyberSecurity (WiCyS) in its mission to help build a strong and gender-balanced cybersecurity workforce. Initiated in 2013 by Dr. Ambareen Siraj through a National Science Foundation (NSF) grant to Tennessee Tech University, WiCyS is now a non-profit organization with a global footprint offering many membership, sponsorship and collaboration benefits.

Learn more about participating, sponsoring and partnering with WiCyS by contacting info@wicys.org.