

LEARNING & PERFORMANCE RESEARCH CENTER, WASHINGTON STATE UNIVERSITY -
PULLMAN

VICEROY Northwest Institute for CyberSecurity Education and Research (CySER). Year 3 Evaluation



Dr. Olusola Adesope
Blessing Akinrotimi

June 2024

Contents

Background.....	2
Year 3 Outcome Achievements	2
Fall 2023 Seminar	3
Method:.....	3
Participants' Demographics:.....	4
Key Findings:.....	4
Participants' Satisfaction:	4
Seminars' Effectiveness in Promoting Learning:	6
Positive Feedback:	7
Spring 2024 Seminar.....	7
Method:.....	7
Participants' Demographics	8
Key Findings:.....	8
Participants' Satisfaction:	8
Seminars' Effectiveness in Promoting Learning:	9
Positive Feedback:	10
Cybersecurity Education and Research Summer 2024 Workshop.....	11
Method:.....	11
Activity Implementations and Key Findings:	12
Activity for Week 1:	12
Activity for Week 2:	13
Key Findings:.....	13
Overall Feedback on the Workshop Satisfaction:.....	17
Recommendations for future workshops:	17
Appendix A.....	18
Appendix B	22

VICEROY Northwest Institute for CyberSecurity Education and Research (CySER) Evaluation Report

Background

The Department of Defense funded the establishment of the VICEROY Northwest Institute for CyberSecurity Education and Research (CySER) – to train cybersecurity ROTC and DoD-skilled civilian workforce. Washington State University leads CySER and collaborates with three other universities: University of Idaho, Montana State University, and Central Washington University.

Year 3 Outcome Achievements

The External Evaluator, Dr. Olusola Adesope, mostly attended meetings with the investigators to discuss overall project goals, examine what is going well and what needs improvements. Data captured during the meetings and reports generated through Qualtrics surveys developed by the external evaluator and administered to participants informed this evaluation report. The report features the Fall seminars, Spring seminars, and the Annual summer workshop. More specifically, the goal of this evaluation report is to examine the extent to which the project has successfully met its objectives for the third year. Additionally, it aims to determine how well positioned the project is for the upcoming year.

Listed below are the major achievements of the project in year 3:

- Seminar series were held biweekly in Fall 2023 (6 seminars) and Spring 2024 (6 seminars). The PI team made considerable efforts to advertise the seminars broadly, and they were well-attended (an average of 36 attendees per seminar). The external evaluation team attended the seminar series and observed robust intellectual and practical discussions at those seminar series.
- Successful recruitment of 11 ROTC members into the program.
- Successful recruitment of 34 Civilian members into the program.
- Successful recruitment of students from various majors, including Computer Science, Cybersecurity, Management Information Systems, and Social Sciences.
- A two-week summer workshop was successfully held on the WSU Pullman campus. The workshop was well attended and included three field trips. Detailed information regarding the workshop is provided later in this report.

- Ten undergraduate students were successfully placed or offered cybersecurity internship opportunities this summer.
- Twenty undergraduate students were involved in cybersecurity projects at varying levels.
- Many graduate research assistants served as mentors to undergraduates.
- There is a great deal of underrepresented minority participation in the program, with Asians, Hispanics, African Americans, and female samples well-represented.

Overall, the project achieved its objectives, and outcomes were successful for Year 3.

Fall 2023 Seminar

The Fall 2023 seminar series featured six presentations on cybersecurity research, education, and career development topics. The seminars were:

- Seminar 1: Securing Critical Infrastructure – Who is CISA and How Can We Help?
Daniel Brown (CISA)
- Seminar 2: The Darkening Tide of Digital Repression and the Risks of Journalistic Reluctance
Jennifer Henrichsen (WSU)
- Seminar 3: Exploring Web-Based Privacy-Invasive Attacks
Xu Lin (WSU)
- Seminar 4: My Journey Through IT and Cybersecurity
Shaun Marquardt (Office of the Washington State Auditor)
- Seminar 5: Cryptography in the Presence of Quantum Computing
Feng-Hao Liu (WSU)
- Seminar 6: Hardware Security.
Shih-Lien Lu (WSU)

Method:

The Fall 2023 seminar series featured six presentations and was held on the following dates: September 18, October 9, October 16, October 30, November 13, and November 27. Attendance at the seminar ranged from a minimum of 28 participants to a maximum of 48, with an average of 40 participants. This indicates a strong and consistent turnout among the undergraduate students, graduate students, and faculty who attended the seminar. The participants were from Washington State University, Montana State University, and Central Washington University. Their majors include Cybersecurity, Computer Science, Mechanical Engineering, Linguistics, Management Information Science, and Analytics & Finance. On average, 65% identify as males and 35% as females. Additionally, 65% identify as White/Caucasian, 21% identify as Asian, 10% identify as Hispanic, and 4% identify as Native Hawaiian or Pacific Islander. Refer to Figures 1 and 2 for participants' gender and ethnicity. At the end of each seminar, participants were asked to complete a survey to provide feedback on different aspects of the presentation.

Participants' Demographics:

Figure 1: Fall 2023 Seminar Series - Participants' Gender

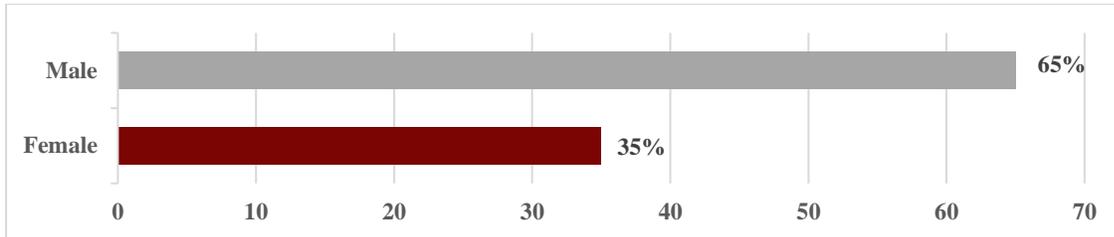
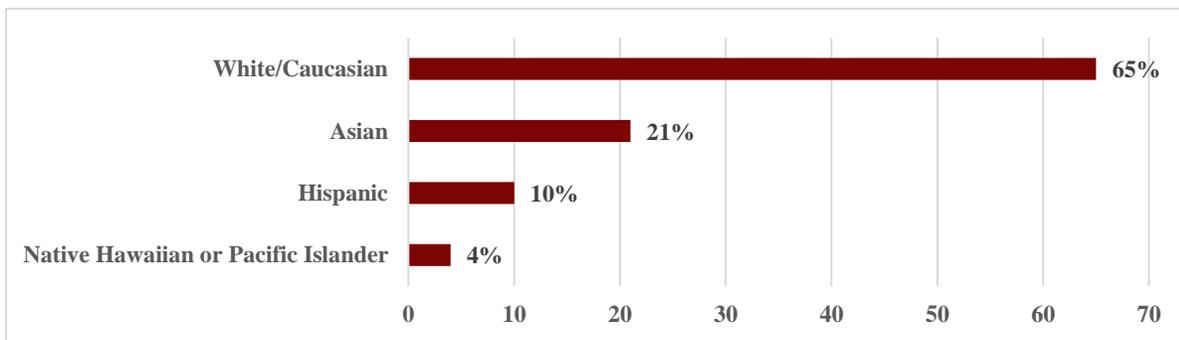


Figure 2: Fall 2023 Seminar Series - Participants' Ethnicity



Key Findings:

Participants' Satisfaction:

Participants were asked to rate their overall satisfaction with the seminar, ranging from extremely satisfied to extremely dissatisfied. Across the six seminars, results consistently indicated high satisfaction among the attendees. On average, about 91% of the participants expressed being somewhat satisfied or extremely satisfied. Refer to Figures 3 & 4 for an overview of the overall satisfaction and individual satisfaction ratings across the spring seminar series.

Figure 3: Fall 2023 Seminar Series - Participants' Overall Satisfaction

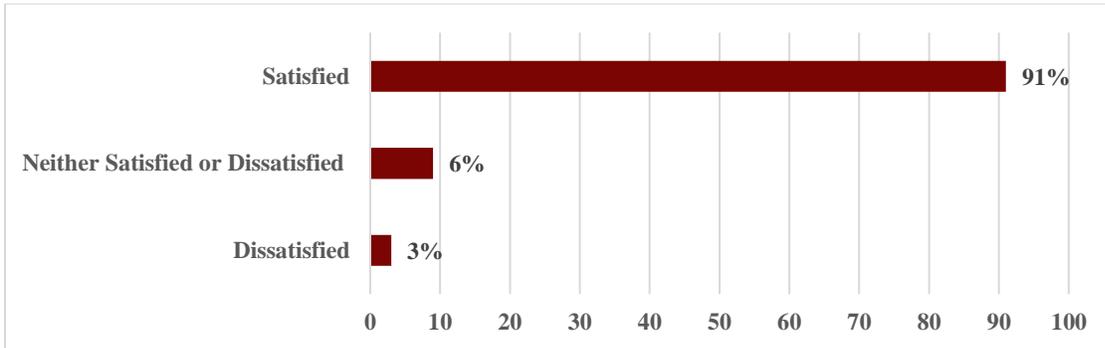
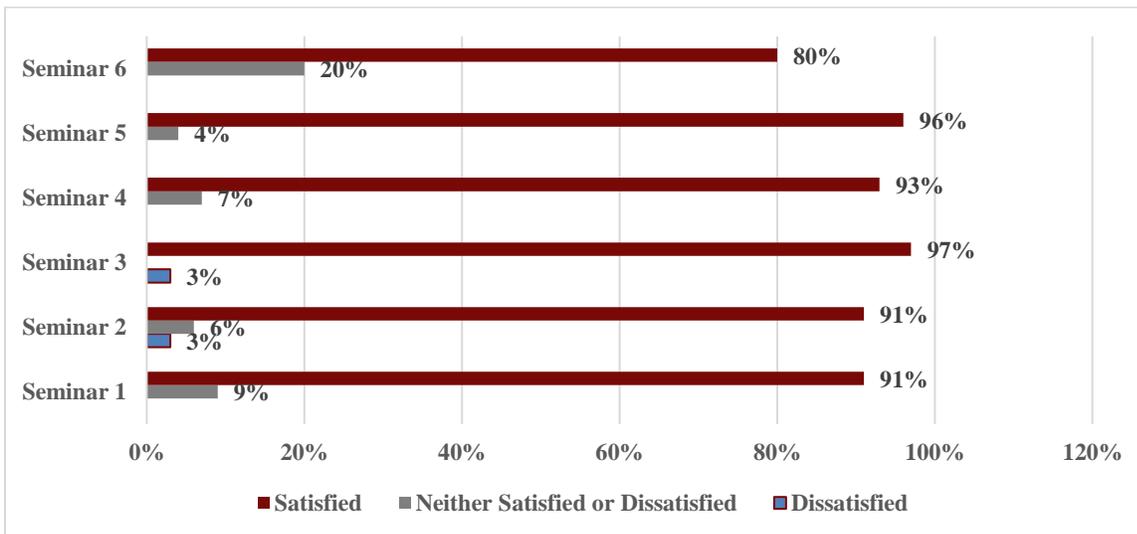


Figure 4: Fall 2023 Seminar Series - Participants' Satisfaction Across Six Seminars



Seminars' Effectiveness in Promoting Learning:

Another important aspect evaluated was the seminars' effectiveness in promoting learning about cybersecurity concepts. Participants rated the effectiveness of the presentation from very high to very low. The seminars successfully promoted the learning of cybersecurity concepts, with 76% indicating somewhat high or high effectiveness. See Figures 5 and 6 for overall and individual effectiveness ratings across the six seminar series.

Figure 5: Fall 2023 Seminar Series - Participants' Overall Rating of Effectiveness

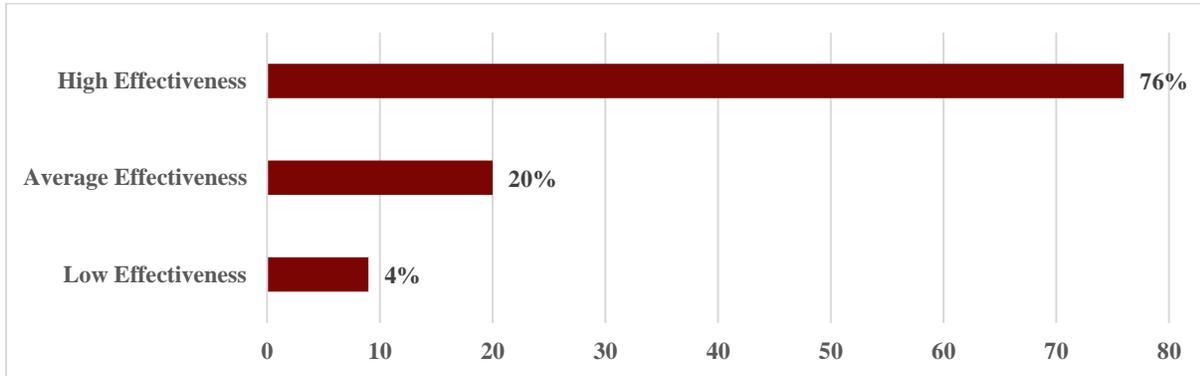
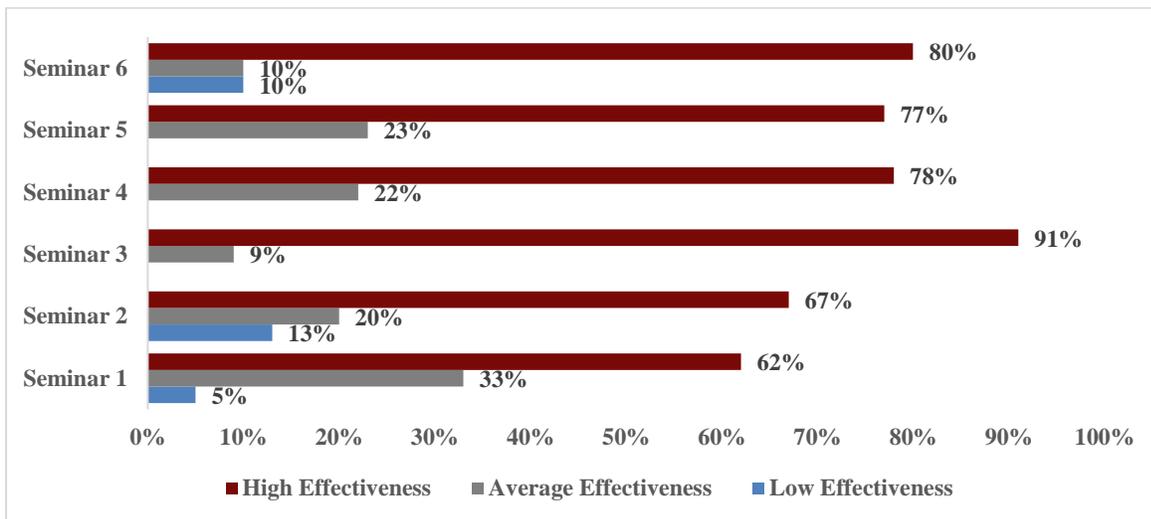


Figure 6: Fall 2023 Seminar Series - Participants' Rating of Effectiveness Across Six Seminars



Positive Feedback:

Participants' feedback indicated that the seminar sessions helped facilitate their understanding of cybersecurity concepts. They lauded the seminars' real-world relevance, career guidance, and technical and advanced topics. Many highlighted the value of using demos and visual aids to explain advanced cybersecurity concepts as they enhanced their understanding. Likewise, others appreciated the presenters' ability to communicate the concepts clearly.

Spring 2024 Seminar

The Spring 2024 seminar series featured six presentations:

- Seminar 1: Industrial Cybersecurity: Ask Different Questions
Andrew Ginter (Waterfall Security Solutions)
- Seminar 2: Why Bits Takes Bytes out of Your Mission
Erich Devendorf (AFRL)
- Seminar 3: Hierarchical Software Quality Assurance
Clemente Izurieta (MSU)
- Seminar 4: Mathematics for Cyber Security
Emilie Purvine (PNNL)
- Seminar 5: Interprocedural Binary Analysis
Matt Revelle (MSU)
- Seminar 6: From Phishing to Floods: Effective and Timely Risk Communication
Messages are Imperative.
Ann Marie Reinhold (MSU)

Method:

The Spring 2024 seminar series featured six presentations and was held on the following dates: February 5, February 19, March 4, March 18, April 1, and April 15. Each seminar had between 22 and 56 attendees. Participants included undergraduate students, graduate students, and principal investigators from participating institutions. There was an average of 43 participants in each seminar session. The minimum number of participants was 28, and the maximum number of participants was 56. On average, twenty ($n = 20$) participants filled out and completed the survey. The participants were from Washington State University, Montana State University, and Central Washington University. Their majors include Cybersecurity, Computer science, Mechanical Engineering, Linguistics, Management Information Science, and Analytics & Finance. On average, 55% identify as Male, 43% as Female, and 2% as other. Additionally, 73% identify as White/Caucasian, 15% identify as Asian, and 12% identify as Hispanic. Refer to Figures 7 and 8 for participants' gender and ethnicity. At the end of each seminar, participants were asked to complete a survey to provide feedback on different aspects of the presentations. The survey consisted of 17 open-ended, closed-ended, and demographic questions. This report

summarizes participants' knowledge about cybersecurity concepts and students' feedback on their experiences during the seminars.

Participants' Demographics

Figure 7: Spring 2024 Seminar Series - Participants' Gender

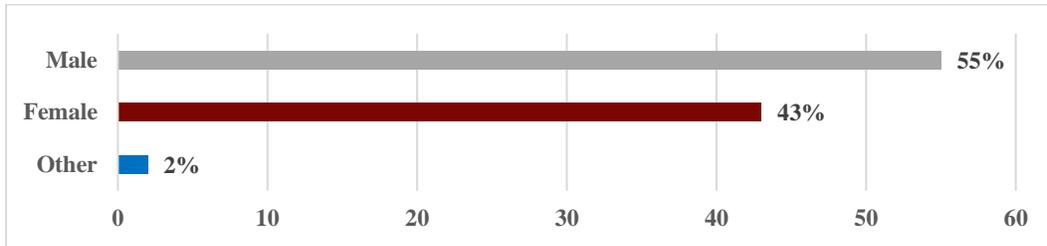
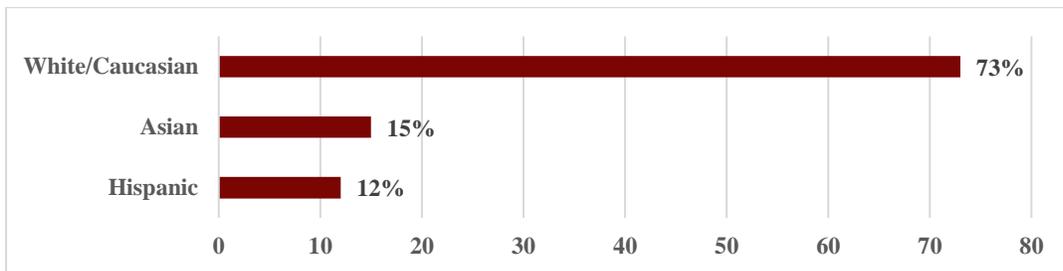


Figure 8: Spring 2024 Seminar Series - Participants' Ethnicity



Key Findings:

Participants' Satisfaction:

Findings across the six seminars indicated that 90% of the respondents expressed being somewhat or extremely satisfied. Specifically, about 63% of the respondents expressed being extremely satisfied, while 27% indicated being somewhat satisfied. See Figures 9 and 10 for an overview of the overall satisfaction and individual satisfaction ratings across the spring 2024 seminar series.

Figure 9: Spring 2024 Seminar Series - Participants' Overall Satisfaction

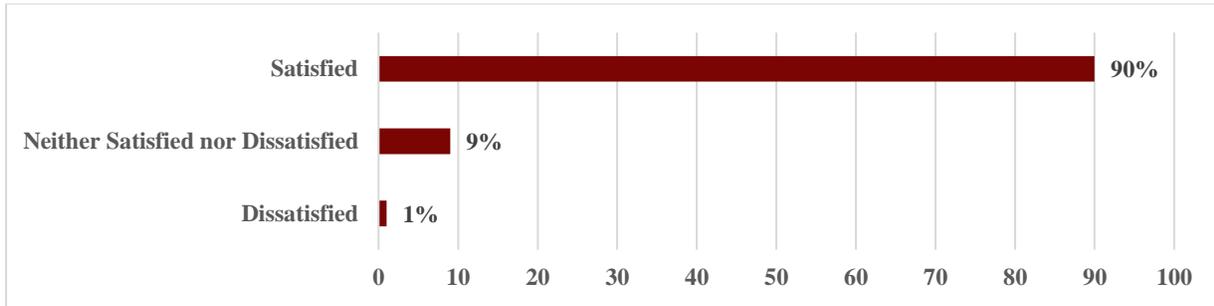
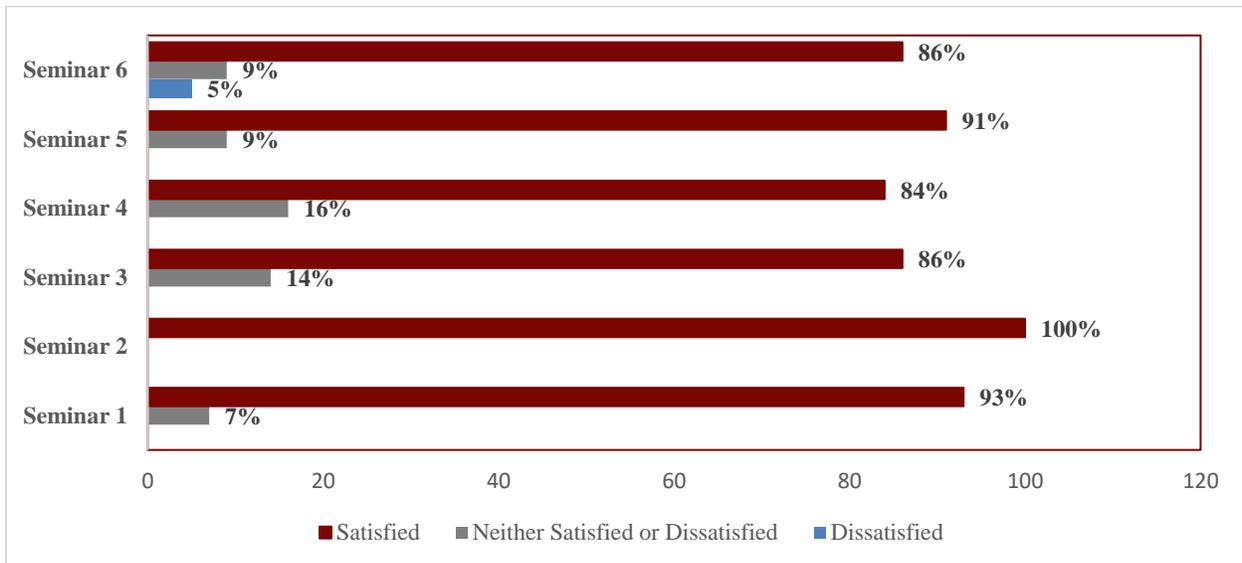


Figure 10: Spring 2024 Seminar Series - Participants' Satisfaction Across Six Seminars



Seminars' Effectiveness in Promoting Learning:

Another important aspect evaluated was the seminars' effectiveness in promoting learning about cybersecurity concepts. Participants rated the effectiveness of the presentation ranging from very high to very low. The seminars successfully promoted the learning of cybersecurity concepts, with 82.83% indicating somewhat high or high effectiveness. Specifically, 54.5% indicated high effectiveness, while 28.33% indicated somewhat high effectiveness. See Figures 11 and 12 for overall and individual effectiveness ratings across the six seminars.

Figure 11: Spring 2024 Seminar Series - Participants' Overall Rating of Effectiveness

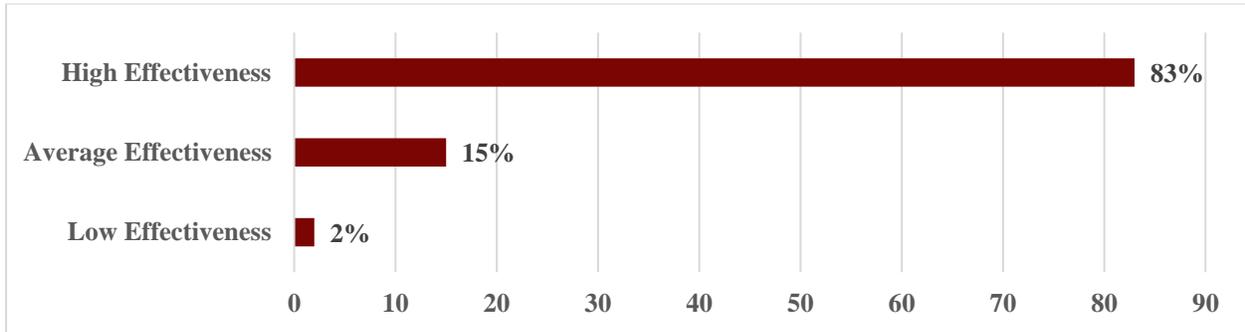
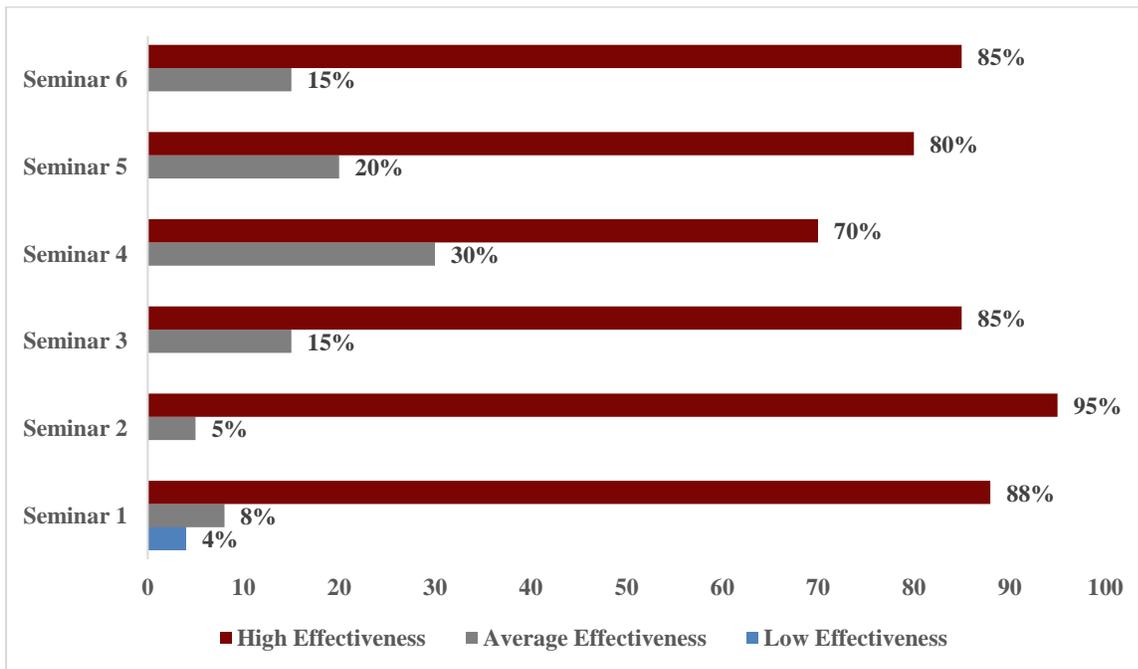


Figure 12: Spring 2024 Seminar Series - Participants' Rating of Effectiveness Across Six Seminars



Positive Feedback:

Across the six seminars, most participants were satisfied with the seminars and agreed that they enjoyed the sessions. Participants also liked how the seminars provided applied or practical cybersecurity examples and occasionally highlighted future career opportunities in cybersecurity within the industry, government, and military sectors. Many highlighted the value of using demos and visual aids to explain advanced cybersecurity concepts as it enhanced their understanding. In addition, others appreciated the presenters' ability to communicate the concepts clearly and their in-depth knowledge of the contents. Participants also indicated that the

seminars were interactive and engaging. Specifically, 90% of the participants strongly agreed that seminar two on “*Why Bits Takes Bytes out of Your Mission*” was very interactive. Survey questions for the Fall 2023 and Spring 2024 seminar series are enclosed in Appendix B of this report.

VICEROY Northwest Institute for CyberSecurity Education and Research (CYSER) Summer 2024 Workshop

The workshop provided training that integrated cybersecurity research and education with professional teamwork, communication, leadership, and lifelong experiential learning. The workshop featured various presentations, lectures, career developments, and hands-on experiential learning activities on cybersecurity topics. In addition, the workshop featured three field trips: a half-day trip to Schweitzer Engineering Laboratories (SEL), a full-day trip to Pacific Northwest National Laboratory (PNNL), and a full-day trip to Fairchild Air Force Base.

Method:

The external evaluator collected data to measure the workshop’s effectiveness through a survey of the participants. Specifically, the survey sought to evaluate participants’ experiences and perceptions of the two-week workshop held at Washington State University Pullman from May 19 to May 29. The external evaluation team collected data via Qualtrics at the end of the two-week workshop to evaluate participants’ overall experiences and the workshop’s effectiveness (please see Appendix A of this evaluation for the workshop survey). On the last day of the workshop, all participants were provided a link to the survey. The survey included Likert-scale, semi-structured, focused questions, and open-ended questions.

There was an average of 30 participants in each workshop session. Twenty-seven ($n = 27$) participants filled out and completed the survey. Participants were from Washington State University (WSU), Montana State University (MSU), and Central Washington University (CWU). Participants’ majors included Computer science ($n = 13$), Cybersecurity ($n = 5$), Management Information Systems ($n = 6$), Linguistics ($n = 1$), Mechanical Engineering ($n = 1$), and Unknown ($n = 1$). Of the participants, 67% identify as Male, 33% identify as Female. Additionally, 67% identify as White/Caucasian, 19% identify as Asian, 11% identify as Hispanic, 7% as Native Hawaiian/Pacific Islander, and 4% identify as Black or African American. Refer to Figures 13 and 14 for participants’ gender and ethnicity.

Figure 13: Summer 2024 Workshop - Participants' Gender

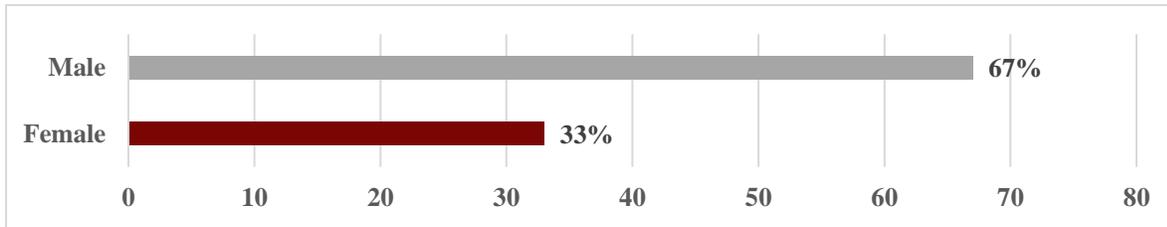
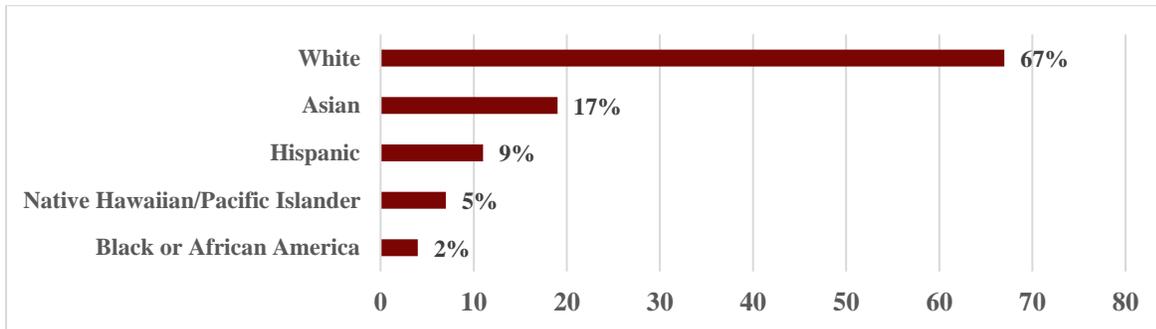


Figure 14: Summer 2024 Workshop - Participants' Ethnicity



Activity Implementations and Key Findings:

The workshop activities were designed to foster experiential learning while remaining aligned with the program's overarching goals.

Activity for Week 1:

The workshop was held in person, with the option for virtual participation. The following activities/lectures took place during the first week of the workshop:

- CySER's Overview and WSU's Commitment to Cybersecurity
- Opportunities at Cybersecurity and Infrastructure Security Agency (CISA)
- Cybersecurity Education in the United States
- Intro to Cybersecurity and Behavioral Threats
- Cybersecurity Career in DoD
- Power Systems and Cybersecurity
- AI, Cybersecurity, and You
- Industrial Control System Cybersecurity Risk Management
- Digital Forensics (Hands-on Demo)
- Operations and Opportunities at NUWC Keyport
- Recent Progress in Modern Cryptography
- Ethics in Cybersecurity

- Human-in-the-Loop Learning Framework for Anomaly Discovery
- Web Browser Fingerprinting: Revealing Stealth Tracking Techniques and Defenses
- Using AI Tools in Cybersecurity (Hands-On Demo)

In addition to various presentations, the workshop included opportunities for students to showcase their work through 16 poster presentations. Of these, 11 were from WSU, 4 were from MSU, and 1 was presented by WSU's cybersecurity club. Certificates were also awarded to acknowledge various accomplishments. In addition, the field trips enhanced experiential learning and practical knowledge.

Sub Activity 1-1:

- Field trips: Schweitzer Engineering Labs and Pacific Northwest National Laboratory
- Track: Team building & leadership
- Students: Poster Presentations and Certificate Ceremony for CySER Graduates.

Activity for Week 2:

The following activities/lectures were held in week 2:

- Protecting Actuators in Real-Time Cyber-Physical Systems
- Empowering learning-based vulnerability analysis via automated augmentation
- Practical Adversarial Malware Attacks and Defenses
- Making the Most of Your Internships

Some additional activities included Field trips and Panel Discussions.

Sub Activity 2-1:

- Field trip to Fairchild Air Force Base
- Cybersecurity Industry Panel Discussion

Key Findings:

The survey responses of participants were evaluated using descriptive analysis. Findings showed that about 65% of the respondents indicated that they learned a lot/a great deal from attending the workshop. About 25% of the respondents stated they gained moderate experiential learning from attending the workshop, while about 9% indicated little learning experience about Cybersecurity.

Overall, the results showed that the workshop was effective, as indicated by the respondent's evaluation of the topics/activities presented during the workshop. Figure 15 shows the percentage of students who rated each workshop activity as being highly effective at promoting their learning of cybersecurity concepts.

Response to topics/activities during the workshop:

The first part of the survey measured the extent to which participants learned from various topics and activities. Most participants indicated that they learned a lot/a great deal on the topics presented at the workshop. For example, on the topic "Industrial Control System Cybersecurity

Risk Management,” 78% indicated that they learned a lot/a great deal from attending the workshop, and 22% indicated a moderate learning experience.

Further analysis of the result indicated that most participants learned a lot/a great deal on topics such as Web Browser Fingerprinting: Revealing Stealth Tracking Techniques and Defenses (78%), Opportunities at CISA (78%), Intro to Cybersecurity and Behavioral Threats (74%), AI, Cybersecurity, and You (74%), Cybersecurity Careers in DoD (74%) and Power Systems and Cybersecurity, (70%).

Participants indicated that they learned moderately on topics such as Protecting Actuators in Real-Time Cyber-Physical Systems (63%), Cybersecurity Education in the United States (63%), Making the Most of your Internship (59%), Recent Progress in Modern Cryptography (59%), Human-in-the-Loop Learning Framework for Anomaly Discovery (56%), Practical Adversarial Malware Attacks and Defenses (56%), Operations and Opportunities at NUWC Keyport (52%) and Empowering Learning-based Vulnerability Analysis via Automated Augmentation (52%).

Specifically, hands-on experiences and team-building activities resulted in higher and more engaging learning experiences for participants. For example, 89% reported moderate to great learning for the Hands-on Tutorial on Digital Forensics. Likewise, 70% indicated they learned a great deal or moderately during the Hands-on Demo on Using AI Tools in Cybersecurity, and 78% indicated they learned a great deal or moderately during the Team Building and Leadership activities.

Also, students and graduate mentors presented their research work during the workshop, and about 88% of the participants indicated that it fostered their learning experience of cybersecurity concepts. All the students indicated that the panel discussion enhanced their understanding of the cybersecurity industry.

These results suggest that hands-on learning, career development, collaborative learning (team building), and panel discussion fostered students’ learning experiences in cybersecurity education and research. Therefore, it is highly recommended that stakeholders, educators, and policymakers provide students with activities that stimulate learners’ interest in cybersecurity education.

Response to Activity Relating to Field Trips:

Participants visited the Pacific Northwest National Laboratory (PNNL), Schweitzer Engineering Lab (SEL), and Fairchild Air Force Base during the workshop. After the trip, participants were asked the extent to which the field trip and outing enhanced their experience. Results showed that 78% indicated that the field trip to SEL enhanced their learning experience because they learned a lot/a great deal visiting SEL. About 11% indicated that they had a moderate learning experience.

The results from the second trip to PNNL showed that 93% of the respondents found the trip beneficial to their learning experience, as they indicated learning a lot or a great deal. About 4% of the respondents stated they had a moderate learning experience from the trip.

The students completed the survey before their third field trip to Fairchild Air Force, so the participants' experiences during that trip were not evaluated.

Measuring the Effectiveness of the Workshop:

Participants were asked to rate the overall effectiveness of the workshop (presentations, lectures, track activities, field trips, poster presentations, and other activities) in promoting their learning about cybersecurity. They responded to five Likert scale questions ranging from very low to very high. The highest score indicates that the workshop effectively promotes participants' learning experiences about cybersecurity education.

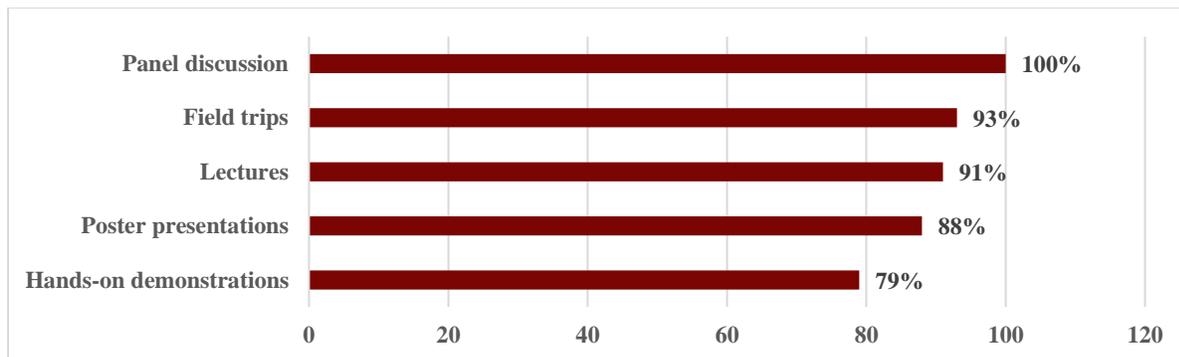
The survey indicated that 81% of the respondents found the workshop to be very/somewhat effective in promoting their learning about Cybersecurity, and 19% indicated that, on average, the workshop was effective in promoting their learning experiences. Furthermore, all the respondents agreed that the workshop's effectiveness was high/average in promoting their learning experiences. Overall, these findings showed that the workshop was beneficial and effective in enhancing learners' experience in cybersecurity education and research.

Also, participants were asked to rate the value they received, considering the time spent attending the workshop. A significant majority, 78% of the respondents, indicated that the workshop was valuable to their learning experience and time spent attending it, while 15% rated the value they received from the workshop as average. Only 7% indicated that the value they received was low, considering the time spent attending the workshop and their learning experiences.

Furthermore, participants were asked open-ended questions to uncover the workshop's effectiveness and if what they learned aligned (or not) with their goals for the workshop. Participants valued the exposure to cybersecurity and how the field trips, career development sessions, and interactive sessions enhanced their learning experience. They appreciated the insights into the cybersecurity career field and its expectations. For instance, one participant stated, *"I think I learned what I need to do to learn more about cybersecurity and the knowledge of what recruiters are looking for."* Others desired the workshop to emphasize practical experiences and examples within the cybersecurity industry. They stated that *"I was hoping to see the current state of cybersecurity in our world, and also look at the tools that we can start to learn and create and protect our system"* and *"They did not go into the practical specialized experience, but I wish I had more of those experiences in the workshop."*

Overall, most participants indicated that **the workshop activities, field trips, lectures, and poster presentations aligned with their goals and expectations for the workshop.**

Figure 15: Summer 2024 Workshop - Participants' Rating of Effectiveness



Findings on Three Key Things Learned from the Workshop:

There are differences in participants' choices regarding the three most valuable things they learned from the workshop. However, most participants indicated that they learned more from the practical hands-on activities, introduction to cryptography, and cybersecurity workforce/career development from presentations, panels, and field trips.

Suggestions for How Future Workshops Could be Improved:

Most participants strongly agreed that the workshop sessions facilitated their learning experience in cybersecurity education and research. However, the following suggestions were made to improve the learning experience in future workshops.

1. More hands-on tutorials and fewer lecture-style presentations from cybersecurity professionals.
2. More collaborative sessions during learning activities
3. More in-person lectures, as virtual presentations, were not interactive.
4. More interactive learning during the lecture-style presentations

Here are a few comments from participants:

- *"More teamwork activities so members can get to know each other better."*
- *"Maybe break activities up so we aren't so disengaged? Put more interactive demos/lessons in between lecture-style presentations."*
- *"I think more hands-on showing of tools that we can start learning from microcontrollers, to reverse engineering, to digital forensics,"*
- *"More hands-on demos that are better prepared so everyone can follow along."*
- *"I would say, put less focus on the research that is being done and put more focus into practical skills and applications of those skills."*

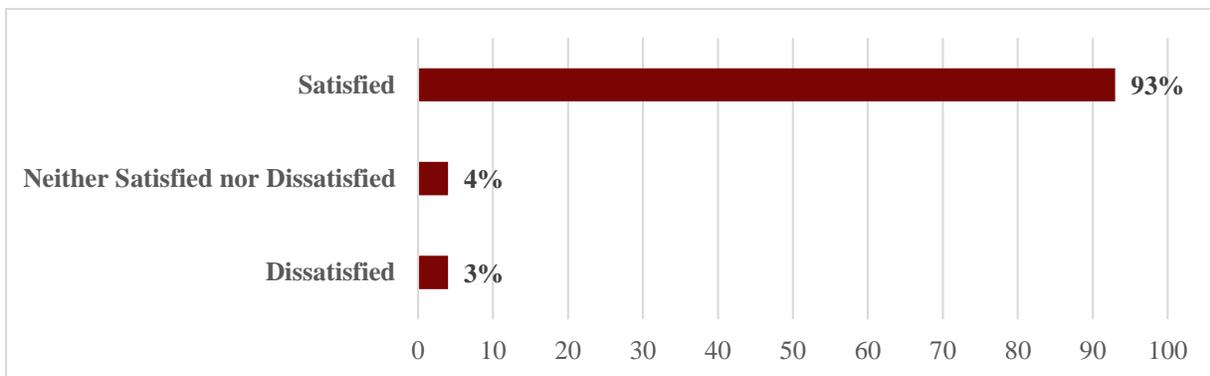
Most participants **recommended introducing more hands-on activities and more in-person presentations** in future workshops.

Overall Feedback on the Workshop Satisfaction:

Participants were asked to rate their level of satisfaction regarding the variety of topics presented at this workshop. Most participants felt strongly satisfied with the variety of topics presented at the workshop. About 93% indicated that they were satisfied/somewhat satisfied with the variety of topics presented at the workshop. About 4% were dissatisfied with the topics presented at the workshop. See Figure 16 for the overall satisfaction of participants during the Workshop.

Overall, participants were satisfied with the contents, presentations, trips, lectures, and workshop quality.

Figure 16: Summer 2024 Workshop - Participants' Satisfaction



Recommendations for future workshops:

First, we want to commend the investigators and key personnel for their excellent work on the project. Most of the recommendations from the past year were reflected in this year's implementation. And though the survey evaluation showed that the workshop was effective and valuable in promoting learners' experience in cybersecurity education and research, we recommend the following be done to strengthen future workshops:

- a. Introduce more hands-on learning activities and implement practices to enhance learners' practical application and understanding of the theoretical components of cybersecurity.
- b. Continue to incorporate more career developments in cybersecurity to encourage prospective students' interest in cybersecurity careers.
- c. Introduce more sessions that promote collaboration and team building among students to optimize learning. This will enhance students' engagement and foster connections with their peers.

Appendix A

Thank you for attending this seminar and for taking the time to leave feedback about your experience. This survey will take approximately 10 minutes.

Q1 Overall, how satisfied are you with the variety of topics presented at this workshop?

- Extremely satisfied
- Somewhat satisfied
- Neither satisfied nor dissatisfied
- Somewhat dissatisfied
- Extremely dissatisfied.

Q2 What did you like **most** about the event?

Q3 What did you like **least** about the event?

Q4 What types of Seminars do you want to see in the future?

- Career Information
- Research-based cybersecurity concepts
- Hybrid – Career and Research-based cybersecurity concepts

Q5 Overall, how would you rate the effectiveness of today's seminar in promoting your learning about cybersecurity concepts?

- Very high
- Somewhat high
- Average
- Somewhat low
- Very low

Q6 What aspect(s) of the seminar did you find particularly helpful?

Q7 Based on your response to the immediate question, could you please explain why the seminar aspect(s) was particularly helpful?

Q8 The seminar was interactive

- Strongly agree
- Somewhat agree
- Neither agree nor disagree
- Somewhat disagree
- Strongly disagree

Q9 Identify three key things you learned from this seminar.

Q10 The length of the seminar was conducive for learning

- Strongly agree
- Somewhat agree
- Neither agree nor disagree
- Somewhat disagree
- Strongly disagree

Q11 Do you have any suggestions for the presenter?

Q12 Do you have any suggestions on how future seminars could be improved

Q13 The University I attend is:

- Washington State University
- Montana State University
- University of Idaho
- Columbia Basin College
- Central Washington University

Q14 Please enter your program level.

- Undergraduate
- Masters
- Doctoral - PhD
- Faculty
- Other

Q15 If undergrad, my major is:

Q16 I am a

- Male
- Female
- Other

Q17 What do you identify as your ethnicity?

- White/Caucasian
- Black or African American
- American Indian or Alaska Native
- Asian
- Native Hawaiian or Pacific Islander
- Hispanic
- Other

Appendix B

Cybersecurity Education & Research Summer Workshop 2024

This is a brief survey of your experience in the 2024 Cybersecurity Education and Research Summer Workshop. The goal of the survey is to solicit feedback on your experience during the workshop. The survey will take about 15 minutes to complete. Responses from the survey will be summarized, and aggregate results will be presented.

We greatly appreciate your time and participation.

Q1 On a scale of 1 to 5 (none at all a great deal), how would you rate how much you learned each of these topics as a result of attending this workshop?

	None at all	A little	A moderate amount	A lot	A great deal
CySER's Overview and WSU's Commitment to Cybersecurity	<input type="radio"/>				
Opportunities at Cybersecurity and Infrastructure Security Agency (CISA)	<input type="radio"/>				
Cybersecurity Education in the United States	<input type="radio"/>				
Intro to Cybersecurity and Behavioral Threats	<input type="radio"/>				
Cybersecurity Career in DoD Power Systems and Cybersecurity	<input type="radio"/>				
AI, Cybersecurity, and You	<input type="radio"/>				
Industrial Control System Cybersecurity Risk Management	<input type="radio"/>				

Q2 On a scale of 1 to 5 (none at all a great deal), how would you rate how much you learned each of these topics as a result of attending this workshop?

	None at all	A little	A moderate amount	A lot	A great deal
Operations and Opportunities at NUWC Keyport	<input type="radio"/>				

Recent Progress in Modern Cryptography	<input type="radio"/>				
Ethics in Cybersecurity	<input type="radio"/>				
Human-in-the-Loop Learning Framework for Anomaly Discovery	<input type="radio"/>				
Web Browser Fingerprinting: Revealing Stealth Tracking Techniques and Defenses	<input type="radio"/>				
Protecting Actuators in Real-Time Cyber-Physical Systems	<input type="radio"/>				
Empowering learning-based vulnerability analysis via automated data augmentation	<input type="radio"/>				
Practical Adversarial Malware Attacks and Defenses	<input type="radio"/>				
Making the Most of Your Internships	<input type="radio"/>				
Army Cyber Command: Defending the Network and the Cloud: Case Studies	<input type="radio"/>				

Q3 On a scale of 1 to 5 (none at all a great deal), to what extent did each of the track activities help you learn in this workshop?

	None at all	A little	A moderate amount	A lot	A great deal
Hand-on Tutorial on Digital Forensics	<input type="radio"/>				
Team Building and Leadership	<input type="radio"/>				
Hands-on Demo: Using AI Tools in Cybersecurity	<input type="radio"/>				

Q4 On a scale of 1 to 5 (none at all a great deal), to what extent did the field trip and outings enhance your experience?

	None at all	A little	A moderate amount	A lot	A great deal
Schweitzer Engineering Labs (SEL)	<input type="radio"/>				
Pacific Northwest National Laboratory (PNNL)	<input type="radio"/>				
Fairchild Air Force Base	<input type="radio"/>				

Q5 To what extent did the panel discussions enhance your experience and understanding of cybersecurity?

- Very high
- Somewhat high
- Average
- Somewhat low
- Very low
-

Q6 To what extent did the poster presentations enhance your experience and understanding of cybersecurity?

- Very high
- Somewhat high
- Average
- Somewhat low
- Very low

Q7 Overall, how would you rate the effectiveness of this workshop in promoting your learning about Cybersecurity (presentations, lectures, track activities, field trips, and other activities)?

- Very high
- Somewhat high
- Average
- Somewhat low
- Very low

Q8 Considering the total investment of your time spent, how would you rate the value you received?

- Very high
- Somewhat high
- Average
- Low
- Very low

Q9 Which aspect(s) of the workshop did you find particularly helpful?

Q10 Based on your response to the immediate question, could you please explain why the workshop aspect(s) was particularly helpful?

Q11 What are three key things you learned from this workshop?

Q12 Could you please explain how those things you learned align (or not) with your goals for the workshop?

Q13 Do you have any suggestions on how future workshops could be improved?

Q14 Overall, how satisfied are you with the variety of topics presented at this workshop?

- Very satisfied
- Somewhat satisfied
- Neither satisfied nor dissatisfied
- Somewhat dissatisfied
- Strongly dissatisfied.

Q15 My name is

Q16 Please enter your program level.

- Undergraduate
- Masters
- Doctoral - PhD
- Faculty
- Other

Q17 If undergrad, my major is:

Q18 I am a

- Male (1)
- Female (2)
- Other (3)

Q19 What do you identify as your ethnicity?

- White/Caucasian
- Black or African American
- American Indian or Alaska Native
- Asian
- Native Hawaiian or Pacific Islander
- Hispanic
- Other

Before you submit, you can modify your answers by clicking the “Back” function Once you click “Next” your responses will be finalized and cannot be changed.