VICEROY Northwest Institute for CyberSecurity Education and Research (CySER).
Year 2 Evaluation

LPRC
Learning and Performance Research Center

Dr. Olusola Adesope
Blessing Akinrotimi

June 2023

Contents

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

Background

The Department of Defense funded the establishment of a Northwest regional VICEROY Virtual Cyber Institute consortium – Cyber Security Education & Research (CySER) – to train cybersecurity ROTC and DoD-skilled civilian workforce. This is led by Washington State University and has other partnering institutions, including the University of Idaho, Hispanic Serving Institution – Columbia Basin College, Montana State University, and Central Washington University.

Year 2 Outcome Achievements

The External Evaluator, Dr. Olusola Adesope, mostly attended biweekly meetings with the investigators to discuss overall project goals, examine what was going well and needed improvements. Data captured during the meetings and reports generated through Qualtrics surveys developed by the external evaluator and administered to research assistants and undergraduate participants informed this evaluation report. More specifically, the goal of this evaluation report is to examine the extent to which the project has successfully met its objectives for the second 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 2:

- With funding from Washington state and catalyzed by VICEROY support, a new Bachelor of Science (BS) in Cybersecurity has been established at WSU and will launch in Fall 2023. The 4-year cybersecurity degree plan is now live, and 120 credits are required for completion of the degree. The first two years are closely aligned to the BS in Computer Science program, and the last two years concentrate on specialized cybersecurity courses.
- The cybersecurity curriculum was approved at all levels as of March 2023, including by the Northwest Commission on Colleges and Universities (NWCCU).
- Seminar series were held biweekly in Fall 2022 (4 seminars) and Spring 2023 (5 seminars). Considerable efforts were made by the PI team to broadly advertise the seminars, and they were well-attended (an average of 29 attendees per seminar). The

external evaluation team attended the seminar series and observed robust intellectual and practical discussions at those seminar series.

- Summer workshop was successfully held for 2 weeks 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.
- Eighteen undergraduate students were successfully placed or offered cybersecurity internship opportunities this summer.
- Twenty-six WSU, four MSU, and four CWU undergraduate students were involved in cybersecurity projects at varying levels.
- Successful recruitment of ROTC members into the project
- Many graduate research assistants serve as mentors to undergraduates.
- There is a great deal of underrepresented minority participation in the program, with Hispanics, African Americans, and females well represented.

Overall, the project achieved its objectives and outcomes were successful for Year 2 and plans for Year 3 are realistic, aligned with project goals, and well-crafted to reach indicated milestones.

Fall 2022 Seminar

The Fall 2022 seminar series featured four presentations on cybersecurity research and education topics. The seminars were:
- Seminar 1: Fall Seminar Series Kick-off: Updates from Partner Institution
  CySER Partner Institutes
- Seminar 2: WebAuthentication: How Passwordless Authentication Works
  Slater Weinstock (Casaba Security)
- Seminar 3: Data and Related Issues in Applying Machine Learning to Cyber Security
  James Halvorsen (WSU)
- Seminar 4: Sustainable Defenses against Evolving Malware in the Android Ecosystems:
 A Manifesto
  Haipeng Cai (WSU)

Method:

The Fall 2022 seminar series featured four presentations and was held on the following dates: October 17, November 14, November 28, and December 12. Participants ranged from 19 to 48 participants at these seminars, including undergraduate students, graduate students, and principal investigators from the participating institutions. The participants were from Washington State University, Montana State University, Columbia Basin College, and Central Washington University. At the end of each seminar, participants were asked to complete a survey to provide feedback on different aspects of the presentation. The data were collected via Qualtrics survey,

which included Likert-scale, open-ended, and semi-structured questions. On average, 79% identify as Males, 11% as Females, and 10% identify as other. Additionally, 64% identify as White/Caucasian, 6% identify as Asian, 20% identify as Hispanic, and 10% identify as other ethnic groups. Refer to Figures 1 and 2 for participants' gender and ethnicity.

Participants' Demographics:

Figure 1: Fall 2022 Seminar Series - Participants' Gender
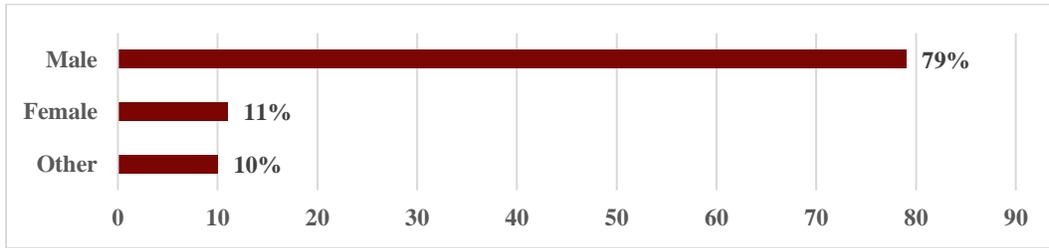
Figure 2: Fall 2022 Seminar Series - Participants' Ethnicity
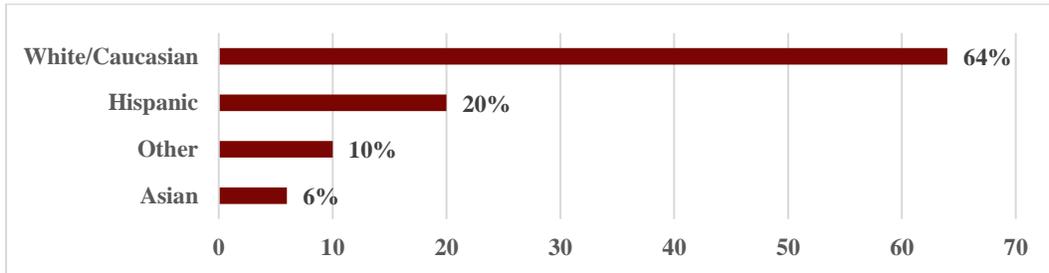
Key Findings:

Participants' Satisfaction:

Participants were asked to rate their overall satisfaction with the seminar, ranging from extremely satisfied to extremely dissatisfied. Across the four seminars, results consistently indicated high satisfaction among the attendees. On average, about 92% of the participants expressed being somewhat satisfied or extremely satisfied, with only 8% being neither satisfied nor dissatisfied. Refer to Figures 3 and 4 for an overview of the overall satisfaction and individual satisfaction ratings across the fall seminar series.

Figure 3: Fall 2022 Seminar Series - Participants' Overall Satisfaction
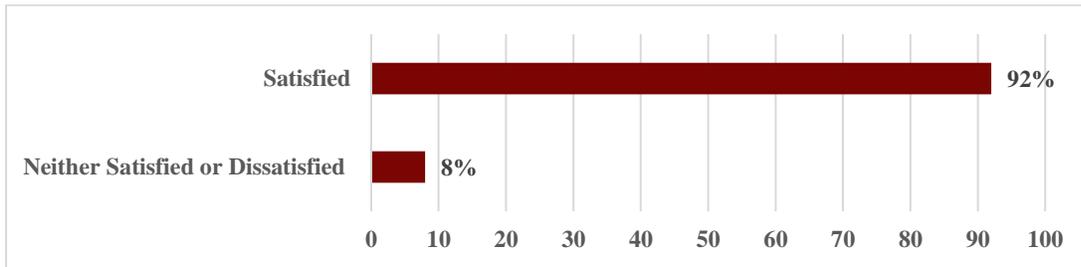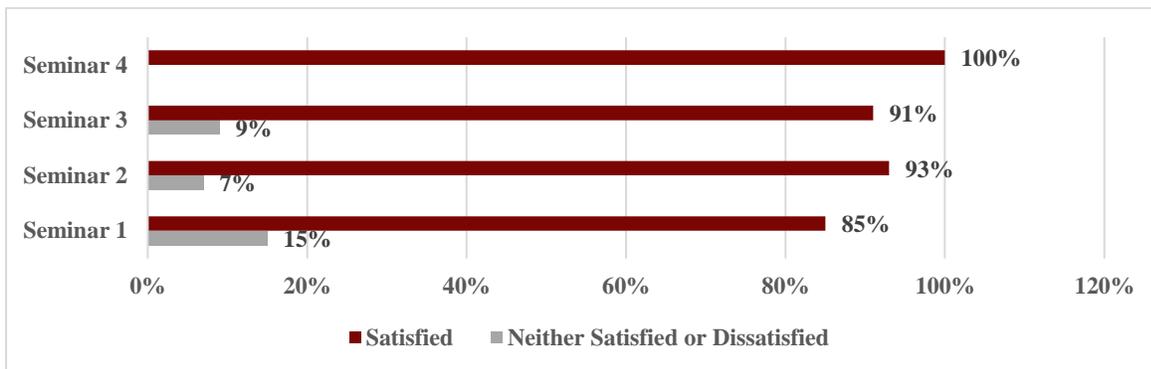

Figure 4: Fall 2022 Seminar Series - Participants' Satisfaction Across Four Seminars

Positive Feedback:

Participants' feedback indicated that they enjoyed the seminar sessions and were highly satisfied with their overall learning experience of cybersecurity content. Students found the seminar informative and praised the presenters for their deep understanding of the material and ability to convey it effectively. Additionally, they valued the opportunity to learn about career prospects in the cybersecurity field.

Spring 2023 Seminar

- Seminar 1: Behavioral Security Research in Information Systems
  Robert Crossler (WSU)
- Seminar 2: Cybersecurity and Quantum Computation in Control of Cyberphysical Systems for Next-Generation Manufacturing
  Helen Durand (Wayne State University)
- Seminar 3: Exploring Platform Reboot as a Security Measure for Cyber-Physical Systems
  Monowar Hasan (WSU)
- Seminar 4: Structural Graph Representation in Learning for National Security Application and Beyond
 Edoardo Serra (Boise State University)

- Seminar 5: Cyber Overview and Opportunities of the Air Force Research Laboratory and Information Directorate
 Sonja Glumich (AFRL/RI – USAF)

Method:

The Spring 2023 seminar series featured five presentations and was held on the following dates: February 6, February 20, March 20, April 3, and April 17. Each seminar had between 22 and 29 attendees. Participants included undergraduate students, graduate students, and principal investigators from participating institutions. The participants were from Washington State University, University of Idaho, Montana State University, Columbia Basin College, and Central Washington University. On average, 76% identify as Male and 24% as Female. Additionally, 71% identify as White/Caucasian, 12% as Hispanic, 15% as Asian, and 6% as other ethnic groups. Refer to Figures 5 and 6 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. Appendix A of this report contains survey questions for the Fall 2022 and Spring 2023 seminar series. This report summarizes participants' satisfaction with the seminar series and students' feedback on their experiences during the seminars.

Participants' Demographics

Figure 5: Spring 2023 Seminar Series - Participants' Gender
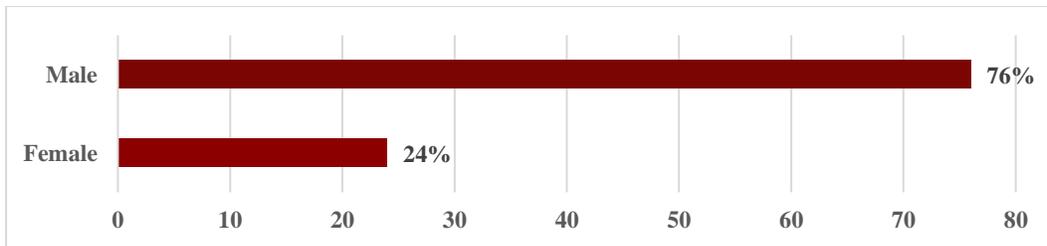
Figure 6: Spring 2023 Seminar Series - Participants' Ethnicity
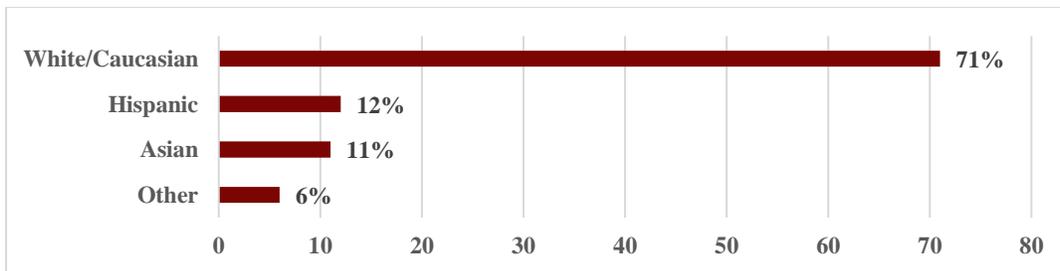
Key Findings:

Participants' Satisfaction:

Findings across the five seminars indicated that 93% of the respondents were somewhat or extremely satisfied. In contrast, less than 4% expressed dissatisfaction with the seminar series. This indicated that the participants were satisfied with the seminar series. See Figures 7 and 8 for an overview of the overall satisfaction and individual satisfaction ratings across the spring 2024 seminar series.

Figure 7: Spring 2023 Seminar Series - Participants' Overall Satisfaction
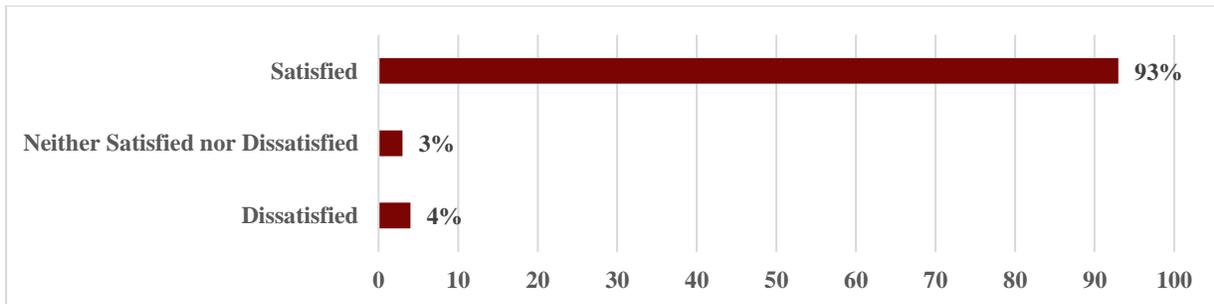
Figure 8: Spring 2023 Seminar Series - Participants' Satisfaction Across Five Seminars
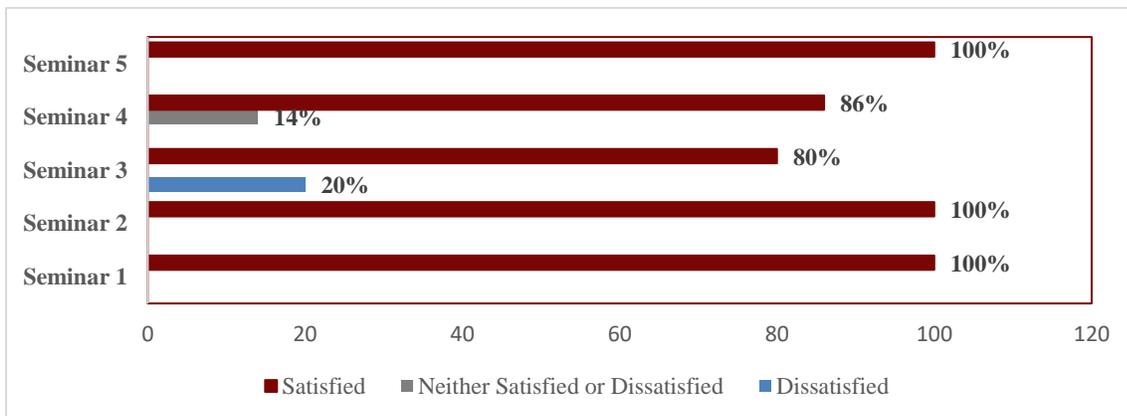
Positive Feedback:

Across the five seminars, most of the participants expressed satisfaction, stating that they enjoyed the sessions and would attend future seminars. They highly rated the presentation style and noted that most presenters were clear, detailed, and knowledgeable. Additionally, all participants agreed that there was ample time for discussions, questions, and answers and that the seminar's duration was conducive to effective learning.

VICEROY Northwest Institute for CyberSecurity Education and Research (CYSER) Summer 2023 Workshop

The workshop aims to provide training that integrates cybersecurity research and education with professional skills in teamwork, communication, leadership, and lifelong experiential learning. The workshop featured various presentations, lectures, career developments, and hands-on experiential learning activities on cybersecurity topics. Besides, 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 22 to June 1. The survey included Likert-scale and semi-structured focused questions such as (i) Which aspect(s) of the workshop did you find particularly helpful?; (ii) What are three key things you learned from this workshop?; (iii) Could you please explain how those things you learned align (or not) with your goals for the workshop?

Prior to the start of the workshop, Dr. Olusola Adesope and his team met with the principal investigator to discuss the best way to assess the workshop. Additional periodic communication via email and Zoom meetings were held to show that the project is underway and activities will occur as planned. The project team met the project's goals and conducted a professional development workshop from May 22 to June 1 on the Washington State University, Pullman campus. 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. See Appendix B for the workshop survey. The survey was developed to assess the workshop's overarching goal. On the last day of the workshop, all participants were provided a link to the survey.

There was an average of 26 participants who attended each workshop session. Of the participants, 14 completed the survey; these 14 participants were from Washington State University ($n = 9$), Montana State University ($n = 2$), Central Washington University ($n = 1$), and Unknown ($n = 2$). Participants' majors include Computer Science ($n = 7$), Engineering ($n = 2$), Conservation Biology and Ecology ($n = 1$), Management Information Science ($n = 1$) and Unknown ($n = 3$). Of the participants, 82% identify as Male, 18% identify as Female. Additionally, 92% identify as White/Caucasian, and 8% identify as Asian. Refer to Figures 9 and 10 for participants' gender and ethnicity.

Participants' Demographics:

Figure 9: Summer 2023 Workshop - Participants' Gender
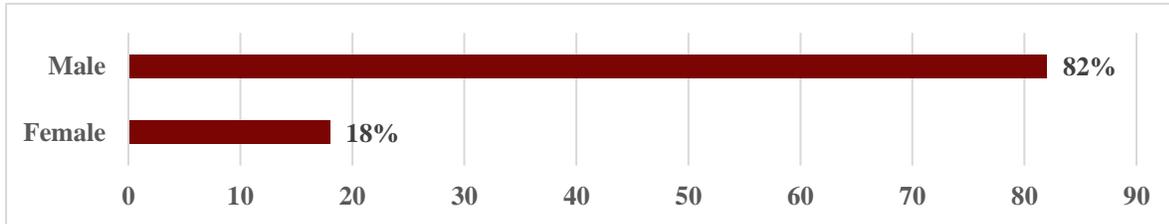
Figure 10: Summer 2023 Workshop - Participants' Ethnicity
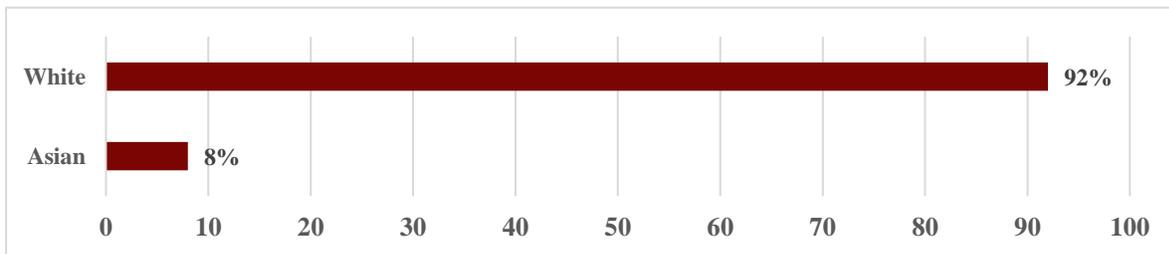
Activity Implementations and Key Findings:
The workshop activities were designed to foster experiential learning while remaining aligned with the overarching objectives of the program.

Activity for Week 1:
The workshop was held in-person with an option for virtual participation. The following activities/lectures took place in the first week of the workshop:
   - Workshop Overview and Generative Machine Learning for Security
   - Legacy System Management and Security
   - Human-in-the-Loop Learning for Anomaly Detection
   - User Interface for Interpretation of Code Vulnerabilities
   - Intro to Cybersecurity and Behavioral Threats
   - Assessing Risks
   - Cyber Overview and Opportunities at AFRL
   - DoD Collaborations and Opportunities
   - Day in the Life of a Cybersecurity Professional
   - Internship Opportunity at the Griffiss Institute – VICEROY Vision
   - Deep Fakes and ChatGPT
   - Graph Mining for Insider Threat Detection
   - Vehicle Cybersecurity
   - Hardware and Malware Detection and Recovery Using FPGAs

- Securing the Supply Chain in a Company
- Army Cyber Command: Defending the Network and the Cloud: Case Studies

In addition to various presentations, the workshop included opportunities for students to showcase their work through poster presentations. Certificates were also awarded to acknowledge various accomplishments. In addition, the track and field trips enhanced experiential learning and practical application.

Sub Activity 1-1:
Field trips: Pacific Northwest National Laboratory and Schweitzer Engineering Labs
Track: Instructional design, Team building & leadership
Students: Poster Presentations and Certificate Ceremony of CySER Graduates.

Activity for Week 2:
The following activities/lectures were held in week 2:

- Power Grid and Cybersecurity
- Cybersecurity in Industrial Control Systems
- Hands-on Tutorial on Digital Forensics
- Cyber Threat Intelligence/Table session
- Simulating Cyber-attacks to Biological Systems: Detection/Mitigation in MATLAB
- Sustainability Defenses Against Evolving Mobile Malware
- Lifelong Learning: Getting the Most Out of Your Internship

Some additional activities included Field trips.

Sub Activity 2-1:
Field trips to Fairchild Air Force Base and Picnic/Hiking

Key Findings:
The workshop was conducted from May 22 to June 1, and each session had an average of 26 participants in each workshop. The survey responses of participants were evaluated using descriptive analysis. Findings showed that about 50.30% of the respondents indicated that they learned a lot/a great deal from attending the workshop. About 31.19% of the respondents indicated that they gained a moderate amount of experiential learning from attending the workshop, while about 16.03% indicated little experience. However, less than 3% responded that the workshop did not influence their 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 11 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 the topics and activities. Most participants indicated that they learned a lot/a great deal about all the topics presented at the workshop. For example, on Assessing Risk, 46.17% indicated that they learned a lot/a great deal from attending the workshop, and 38.46% indicated a moderate learning experience. In comparison, 7.69% indicated little experience.

Further investigations of the result indicated that most participants learned a lot/a great deal on topics such as "Legacy Systems Management and Security (84.62%), Cyber Overview and Opportunities at AFRL (92.31%), DoD Collaborations and Opportunities (84.61%) and Internship Opportunity at the Griffiss Institute – VICEROY Vision (84.62%). Participants indicated that they learned these topics moderately, and they include: Power grid and Cybersecurity (69.23%), Day in Life of a Cybersecurity Professional (69.23%), Team Building and Leadership (61.54%), Workshop Overview and Generative Machine Learning for Security (53.85%). Participants indicated that they learned very little on topics such as "Securing Supply Chain in a company (30.77%), Human-in-the-Loop Learning for Anomaly Detection (30.77%), and User Interface for Interpretation of Code Vulnerabilities (30.77%)

Specifically, hands-on experiences, team-building activities, and career presentations produced higher and more fun learning experiences for participants. Also, students and graduate mentors presented their research work during the workshop, and about 90% of the participants indicated that it fostered their learning experience of cybersecurity concepts.

These results suggest that hands-on learning, career development, and collaborative learning (team building) may foster 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/Picnic/Hiking:

Participants visited Pacific Northwest National Laboratory (PNNL), Schweitzer Engineering Lab (SEL), and Fairchild Air Force Base during the workshop. After the trip, participants were asked about the extent to which the field trip and outing enhanced their experience. Results showed that 91.67% indicated that the field trips and outings enhanced their experience because they learned a lot/a great deal visiting PNNL. About 8.3% indicated that they had a moderate learning experience.

The results from the second trip to SEL showed that 92.31% of the respondents found the trip beneficial to their learning experience, as they indicated learning a lot/a great deal. About 7.7% of the respondents indicated that they had a moderate learning experience from the trip.

The results from the third field trip to Fairchild Air Force Base showed that 83.34% of the respondents found the trip beneficial to their learning experience as they indicated learning a lot/a great lot. While 16.67% of the respondents indicated that they had a moderate learning experience that enhanced their learning experience.

Findings from Kamiak Butte Hiking and Picnic showed that 75% of the respondents found the hiking experience beneficial to their learning, and 16.67% found it moderately interesting.

Measuring the Effectiveness of the Workshop:

Participants were asked to rate the overall effectiveness of the workshop (presentations, lectures, track activities, field trips, 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.

76.92% of the respondents indicated that the workshop was somewhat/very high in promoting their learning about Cybersecurity, and 23.08.8% indicated that, on average, the workshop was effective in promoting their learning experiences. Furthermore, all the respondents indicated 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. 61.54% of the respondents indicated that the workshop was valuable to their learning experience and time spent attending it. 30.77% rated the value they received from the workshop as average. In comparison, 7.69% stated that the value they received was low considering the time spent attending the workshop and their learning experiences.

Additionally, participants were asked five open-ended questions to analyze the workshop's effectiveness and how what they learned aligned (or not) with their goals for the workshop. Participants stated that hands-on learning enhanced their comprehension of cybersecurity education. For instance, a participant stated that "I really liked the hands-on tutorials." Others indicated that the field trips, career development sessions, and interactive sessions also enhanced their learning experience. Participants further explained that the "hands-on tutorial really helped with learning concepts and how they apply to the real world". They also indicated that the field trips "gave practical insights into what a cybersecurity day to day career entails". These comments indicate that hands-on learning and practical sessions enhance learners' understanding of the content learned in cybersecurity and keep them interested in exploring careers in cybersecurity.

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

Figure 11: Summer 2023 Workshop - Participants' Rating of Effectiveness
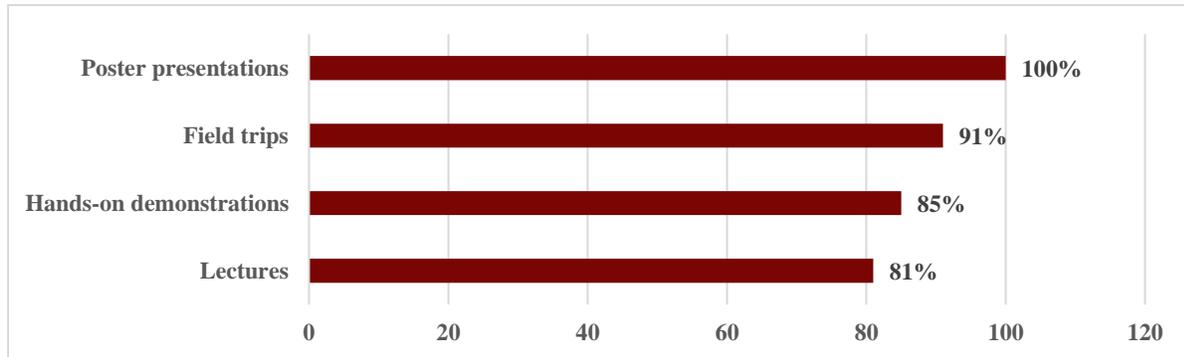
Findings on Three Key Things Learned from the Workshop:
There were differences in participants' choices regarding the three most valuable things participants learned from the workshop. However, most participants indicated that they learned Practical hands-on learning, legacy systems management, and cybersecurity workforce/career development from presentations and field trips. Others indicated that they learned power grid vulnerabilities, risk management, and anomaly detection.

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. Introduction of more techniques used today in Cybersecurity.
2. More hands-on tutorials and fewer lecture-style presentations from cybersecurity professionals.
3. More Field trips to private cybersecurity institutions.
4. More of the sessions were too advanced. Hence, there is a need to provide adequate information on the basics of cybersecurity.
5. More team building sessions.
6. Less time and summer sessions could be condensed into one week.
7. More in-person lectures, as virtual presentations, were not interactive and were distracting.

Here are a few comments from participants:

- *"I believe the workshop could be condensed into a single week instead of taking up two weeks."*
- *"The concepts should be simplified for a more general audience. Introduce concepts with the expectation that not everyone knows anything about what you do."*

- *There were a few lectures that did not actually happen, and all of the ones done over Zoom were really difficult to pay attention to."*
- *"I would also suggest keeping the field trips and possibly increasing them as that is what I learned the most from and was most interested in coming from a non-cyber background."*
- *I think there should be more hands-on tutorials, and the concepts should be simplified for a more general audience. Introduce concepts with the expectation that not everyone knows anything about what you do."*

Most participants **recommended introducing more hands-on activities and 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 this workshop. 90.91% indicated that they were satisfied/somewhat satisfied with the variety of topics presented at the workshop. 9.09% were neither satisfied nor dissatisfied with the topics presented at the workshop. See Figure 12 for the overall satisfaction of participants during the Workshop.

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

*Figure 12: Summer 2023 Workshop **-** Participants' Satisfaction*
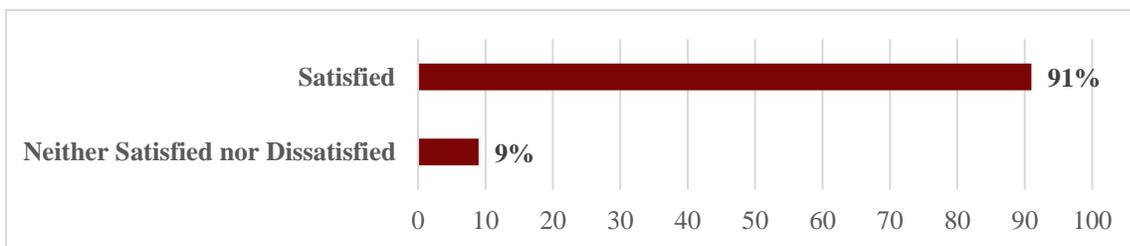
Recommendations for future workshops:

First, we want to commend the investigators and key personnel for their excellent work on the project. Although the survey evaluation showed that the workshop was effective and valuable in promoting learners' experience in cybersecurity education and research, we recommend that the following be done to strengthen future workshops:

a. Introduce more hands-on learning activities and implement engagement practices to leverage learners' 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. Facilitate more sessions on undergraduate and graduate research in cybersecurity and resource optimization. This will help students develop their knowledge and skills in the field.
d. Do more in-person presentations for optimal participation and engagement.

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 How likely are you to recommend this seminar to a friend or college

- ◯ Extremely likely
- ◯ Likely
- ◯ Somewhat likely
- ◯ Not at all

Q2 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.

Q3 What did you like **most** about the seminar?

_____

_____

_____

Q4 What did you like **least** about the seminar?

_____

_____

_____

_____

Q5 What could make the seminar session better?

◯ Better Materials

◯ More interactive activities

◯ Better presentation skills

◯ More room for discussion

Q6 Have you attended any of our seminars before?

◯ Yes

◯ Maybe

◯ No

Q7 Will you join our next seminar?

◯ Yes

◯ Maybe

◯ No

Q8 Would you say the seminar was interactive?

◯ Yes

◯ No

◯ Not sure

Q9 There was enough time for discussions, questions, and answers

◯ Strongly agree

◯ Somewhat agree

◯ Neither agree nor disagree

◯ Somewhat disagree

◯ Strongly disagree

Q10 The length of the seminar was conducive to learning

◯ Strongly agree

◯ Somewhat agree

◯ Neither agree nor disagree

◯ Somewhat disagree

◯ Strongly disagree

Q11 What types of seminars do you want to see in the future? (Career or research-based information on cybersecurity concepts)?

_____

_____

Q12 How can future seminars be improved?

_____

_____

Q13 Is there anything else you would like to share with us?

_____

_____

Q14 The University I attend is:

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

Q15 Please enter your program level.

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

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

Cybersecurity Education & Research Summer Workshop 2023

This is a brief survey of your experience in the 2023 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
Workshop Overview and Generative Machine Learning for Security	❍	❍	❍	❍	❍
Legacy Systems Management and Security	❍	❍	❍	❍	❍
Human-in-the-loop Anomaly Detection	❍	❍	❍	❍	❍
User Interface for Interpretation of Code Vulnerabilities	❍	❍	❍	❍	❍
Intro to Cybersecurity and Behavioral Threats	❍	❍	❍	❍	❍
Assessing Risk	❍	❍	❍	❍	❍
Cyber Overview and Opportunities at AFRL	❍	❍	❍	❍	❍
DoD Collaboration and Opportunities	❍	❍	❍	❍	❍

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
Day-in-the-life of a Cybersecurity Professional	○	○	○	○	○
Internship Opportunity at the Griffiss Institute – VICEROY Vision	○	○	○	○	○
Team Building and Leadership	○	○	○	○	○
Deep Fakes and ChatGPT	○	○	○	○	○
Graph Mining for Insider Threat Detection	○	○	○	○	○
Vehicle Cybersecurity	○	○	○	○	○
Hardware and Malware Detection and Recovery Using FPGAs	○	○	○	○	○
Securing the Supply Chain in a Company	○	○	○	○	○
Army Cyber Command: Defending the Network and the Cloud: Case Studies	○	○	○	○	○
National Cyber League	○	○	○	○	○

Q3 On a scale of 1 to 5 (none at all .... a great deal), how would you rate how much you learned in each of these topics as a result of attending this workshop?

	None at all	A little	A moderate amount	A lot	A great deal
Power Grid and Cybersecurity	❍	❍	❍	❍	❍
Cybersecurity in Industrial Control Systems	❍	❍	❍	❍	❍
Hand-on Tutorial on Digital Forensics	❍	❍	❍	❍	❍
Hands-on Tutorial: Linux Tools for Binary Reverse Engineering	❍	❍	❍	❍	❍
Cyber Threat Intelligence/Table Session	❍	❍	❍	❍	❍
Simulating Cyber-attacks to Biological Systems: Detection/Mitigation in MATLAB	❍	❍	❍	❍	❍
Sustainability Defenses Against Evolving Mobile Malware	❍	❍	❍	❍	❍
Lifelong Learning: Getting the Most Out of Your Internship	❍	❍	❍	❍	❍

Q4 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
Team Building and Leadership	❍	❍	❍	❍	❍
Hand-on Tutorial on Digital Forensics	❍	❍	❍	❍	❍
Hands-on Tutorial: Linux Tools for Binary Reverse Engineering.	❍	❍	❍	❍	❍

Q5 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
Pacific Northwest National Laboratory (PNNL)	○	○	○	○	○
Schweitzer Engineering Labs (SEL)	○	○	○	○	○
Hiking and Picnic	○	○	○	○	○
Fairchild Air Force Base	○	○	○	○	○

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 The university I attend is:

_____

Q17 Please enter your program level.

○ Undergraduate

○ Masters

○ Doctoral - PhD

○ Faculty

○ Other

Q18 If undergrad, my major is:

_____

Q19 I am a

○ Male (1)

○ Female (2)

○ Other (3)

Q20 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