SAINT LOUIS UNIVERSITY.

Program-Level Assessment: Annual Report

Program Name (no acronyms): Cybersecurity	Department: SPS Graduate Programs
Degree or Certificate Level: Master's of Science	College/School: Professional Studies
Date (Month/Year): August/2023	Primary Assessment Contact: Maria Weber
In what year was the data upon which this report is based collected? 2023	
In what year was the program's assessment plan most recently reviewed/updated? 2023	

1. Student Learning Outcomes

Which of the program's student learning outcomes were assessed in this annual assessment cycle? (Please list the actual learning outcome statements and not just numbers, e.g., Outcomes 1 and 2.)

SLO 3: Graduates will be able to construct and implement networks and data management systems that protect intellectual property using cybersecurity principles.

SLO 4: Graduates will be able to apply information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

2. Assessment Methods: Artifacts of Student Learning

Which artifacts of student learning were used to determine if students achieved the outcome(s)? Please identify the course(s) in which these artifacts were collected. Clarify if any such courses were offered a) online, b) at the Madrid campus, or c) at any other off-campus location.

Our new assessment protocol integrates data from three sources to evaluate student learning:
1. Each program LO is mapped to specific courses and artifacts within those courses (see below). Instructors complete an assessment of learning that is attached to the rubric of the artifact's grading rubric. It is important to note that this process is meant to gather data that is independent of grades given.
2. Faculty mentors complete a summative assessment on each student at the conclusion of their capstone. Mentor's assess the student's performance for each of the learning outcomes.
3. A student assessment of learning outcomes is also completed by students at the end of their degree. This indirect measure asks students to rate the extent they learned and developed on each LO. They also indicate what specific competencies they developed and which they feel they need additional development.

Data from individual students and students completing the master's research project (CYBR 5963)
SLO 3: Graduates will be able to construct and implement networks and data management systems that protect intellectual property using cybersecurity principles.

CYBR 5010, Networking Concepts
Spring 2023
CYBR-5010 -12 - 13 students * Final Project
CYBR-5010 -13 - 14 students ** Final Project
CYBR-5010 -14 - 10 students ** Final Project
CYBR-5010 -15 - 9 students ** Final Project

CYBR 5020, Data Administration
Spring 2023

CYBR-5020 - 11- 2 students * Final Project

CYBR 5030, Cyber Threats
Spring 2023
CYBR-5030 - 21 - 18 students* Final Project
CYBR-5030 - 22 - 17 students* Final Project
CYBR-5030 - 23 - 13 student * Final Project

CYBR 5210, Digital Investigations
No Offered

CYBR 5220, Incident Response and Mitigation
Fall 2022
CYBR-5220 - 11 - 6 student * Final Project
CYBR-5220 - 12 - 19 student * Final Project

CYBR 5961/ CYBR 5262/ CYBR 5963 -Master Research Project I/II/III
Spring 2023
CYBR-5961 - 11 - 1 students * Master Research Prospectus
CYBR-5963 - 11 - 9 students * Master Research Project
CYBR-5961 - 21 - 5 students * Master Research Prospectus
CYBR-5963 - 21 - 8 students * Master Research Project
Summer 2022
CYBR-5961 -11 - 2 students* Master Research Project
Fall 2022
CYBR-5963- 21 - 4 students * Master Research Project
CYBR-5962 - 11 - 1 students * Master Research Prospectus
CYBR-5962 - 21 - 2 students * Master Research Prospectus

SLO 4: Graduates will be able to apply information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

CYBR 5010, Networking Concepts
Spring 2023
CYBR-5010 -12 - 13 students * Final Project
CYBR-5010 -13 - 14 students ** Final Project
CYBR-5010 -14 - 10 students ** Final Project
CYBR-5010 -15 - 9 students ** Final Project

CYBR 5020, Data Administration
Spring 2023
CYBR-5020 - 11- 2 students * Final Project

CYBR 5030, Cyber Threats
Spring 2023
CYBR-5030 - 21 - 18 students * Final Project
CYBR-5030 - 22 - 17 students * Final Project
CYBR-5030 - 23 - 13 student * Final Project

CYBR 5230, Intrusion Detection and Analysis
Spring 2023
CYBR-5230- 21 - 6 students * Final Project
CYBR-5230- 22 - 8 students ** Final Project
CYBR-5230- 23 - 10 students ** Final Project
CYBR-5230- 24 - 8 students ** Final Project
CYBR-5230- 25 - 11 students ** Final Project

CYBR 5240, Cloud Security
Summer 2022
CYBR-5240- 11 - 4 students * Final Project

CYBR 5961/ CYBR 5262/ CYBR 5963 -Master Research Project I/II/III
Spring 2023
CYBR-5961 - 11 - 1 students * Master Research Prospectus
CYBR-5963 - 11 - 9 students * Master Research Project
CYBR-5961 - 21 - 5 students * Master Research Prospectus
CYBR-5963 - 21 - 8 students * Master Research Project
Summer 2022
CYBR-5961 -11 - 2 students* Master Research Project

Fall 2022
CYBR-5963- 21 - 4 students * Master Research Project
CYBR-5962 - 11 - 1 students * Master Research Prospectus
CYBR-5962 - 21 - 2 students * Master Research Prospectus

Legend: * Courses were taught 100% online
**Courses were taught 100% on-campus
Note: No courses offered in Madrid Campus

3. Assessment Methods: Evaluation Process

What process was used to evaluate the artifacts of student learning, and by whom? Please identify the tools(s) (e.g., a rubric) used in the process and include them in/with this report.

The artifacts were evaluated by the program director in consultation with the course instructor. The evaluation involved one instructor for each course (i.e., one for CYBR 5000, another for CYBR 5010, etc.) Each artifact is assessed according to a standard rubric in Canvas. Instructors, after grading the artifact, rate the student in terms of their learning mastery. The learning outcome assessment is separate from the grade given on the assignment. We pulled raw survey data from each of the courses. Survey has moved back from Canvas to Qualtrics We then tabulated the quantitative data to provide a high-level overview.

4. Data/Results

What were the results of the assessment of the learning outcome(s)? Please be specific. Does achievement differ by teaching modality (e.g., online vs. face-to-face) or on-ground location (e.g., STL campus, Madrid campus, other off-campus site)?

Results indicated that students meet SLO 3 but are in need of new courses with program-specific knowledge courses to address new practical problems

SLO 3: Graduates will be able to construct and implement networks and data management systems that protect intellectual property using cybersecurity principles.

CYBR 5010, Networking Concepts
Spring 2023
CYBR-5010 -12 - 13 students * Final Project - - 85% Meet Standard and 15 % Do not Meet Standard. Students who did not meet the standards withdrew the course. Students who meet the standard The final project evaluates the criteria as follows students are given a role-play case scenario as a Network Architect who needs to perform a security assessment on the network and design a solution to make a company's network more secure at every layer. Students who met the standard were able to assess and build a secured network. Student who did not perform well did not complete all the requirements

CYBR-5010 -13 - 14 students ** Final Project - 100% Meet Standard . Students who did not meet the standards withdrew the course. Students who meet the standard The final project evaluates the criteria as follows students are given a role-play case scenario as a Network Architect who needs to perform a security assessment on the network and design a solution to make a company's network more secure at every layer. Students who met the standard were able to assess and build a secured network.

CYBR-5010 -14 - 10 students ** Final Project - 91% Meet Standard and 9 % Do not Meet Standard. Students who did not meet the standards withdrew the course. Students who meet the standard The final project evaluates the criteria as follows students are given a role-play case scenario as a Network Architect who needs to perform a security assessment on the network and design a solution to make a company's network more secure at every layer. Students who met the standard were able to assess and build a secured network. Student who did not perform well did not complete all the requirements

CYBR-5010 -15 - 9 students ** Final Project - 100% Meet Standard Students who did not meet the standards withdrew the course. Students who meet the standard The final project evaluates the criteria as follows students are given a role-play case scenario as a Network Architect who needs to perform a security assessment on the network and design a solution to make a company's network more secure at every layer. Students who met the standard were able to assess and build a secured network.

CYBR 5020, Data Administration

Spring 2023

CYBR-5020 - 11- 2 students * Final Project - 100% Meet Standard. Students were able to meet the standard in the Final Project students are asked in a case scenario to propose a company which is currently a non-health care company, but the CEO what technical challenges are present as he is pivoting into the health care sector (and the company would be handling ePHI). Students were able to propose data management systems that robustly protect intellectual property using HIPPA. Students found gaps in the current program that need to be fixed so that they could achieve compliance, and develop a plan to achieve compliance within 1 year and prioritize what can/can not be done, discussing risks if they could not achieve 100% compliance.

CYBR 5030, Cyber Threats

Spring 2023

CYBR-5030 - 21 - 18 students* Final Project - 94% Meet Standard and 6% Approaches Standard During the final project, students act as the newly hired CIO/CISO in an organization that has PCI requirements, a third party vendor to conduct an internal and external pen test per PCI requirements. 94% of the students utilized the PenTest Execution Standard (PTES) for reporting. Students were involved in the pen test as an active stakeholder. As part of this report, students met the standard by reporting on existing network traffic controls,network ranges owned by the organization, and identified possible weaknesses determining the impact of a security breach on confidentiality of the company's information and Internal infrastructure and availability. The 6 % of the students that approached the standard missed an artifact/assignment.

CYBR-5030 - 22 - 17 students* Final Project - 100% Meet Standard During the final project, students act as the newly hired CIO/CISO in an organization that has PCI requirements, a third party vendor to conduct an internal and external pen test per PCI requirements. 96% of the students utilized the PenTest Execution Standard (PTES) for reporting. Students were involved in the pen test as an active stakeholder. As part of this report, students met the standard by reporting on existing network traffic controls,network ranges owned by the organization, and identified possible weaknesses determining the impact of a security breach on confidentiality of the company's information and Internal infrastructure and availability.

CYBR-5030 - 23 - 13 student * Final Project - 87% Meet Standard and 13% Do not meet standard During the final project, students act as the newly hired CIO/CISO in an organization that has PCI requirements, a third party vendor to conduct an internal and external pen test per PCI requirements. 96% of the students utilized the PenTest Execution Standard (PTES) for reporting. Students were involved in the pen test as an active stakeholder. As part of this report, students met the standard by reporting on existing network traffic controls,network ranges owned by the organization, and identified possible weaknesses determining the impact of a security breach on confidentiality of the company's information and Internal infrastructure and availability. The 13% of the students (2) that did not meet the standard due to it withdrew the course.

CYBR 5220, Incident Response and Mitigation

Fall 2022

CYBR-5220 - 11 - 6 student * Final Project - 50% Meet Standard and 50% Approaches Standard. During the final project students prepare a report for the CIO/CISO on an on-going security incident that is being executed against their company from an Eastern European based hacking group. Students provided the following information: How the incident occurred, What happened during the incident, Short term remediations put into place, Long term remediations needed for the roadmap, What a claim needs to be made to our cyber insurance provider or whether we need to send a breach notification (and why) and recommendations of changes need to be implemented to the networks and data management systems to protect intellectual property using cybersecurity principles. Students have to utilize incident response frameworks such as NIST, SANS. 50% of the students met the standard in developing the final project described above. While 50% of students did not develop a full incident report..

CYBR-5220 - 12 - 19 student * Final Project - 100% Meet Standard During the final project students prepare a report for the CIO/CISO on an on-going security incident that is being executed against their company from an Eastern European based hacking group. Students provided the following information: How the incident occurred, What happened during the incident, Short term remediations put into place, Long term remediations needed for the roadmap, What a claim needs to be made to our cyber insurance provider or whether we need to send a breach notification (and why) and recommendations of changes need to be implemented to the networks and data management systems to protect intellectual property using cybersecurity principles. Students have to utilize incident response frameworks such as NIST, SANS. In this section, all student met the standard

CYBR 5961/ CYBR 5262/ CYBR 5963 -Master Research Project I/II/III

Spring 2023

CYBR-5961 - 11 - 1 students * Master Research Prospectus - 100% Meet Standard - All students identified the purpose and scope of the problem they intend to address. This is the first of a 3-sequence course. Students choose a topic to apply cybersecurity best practices to safeguard intellectual property.

CYBR-5963 - 11 - 9 students * Master Research Project - 100% Meet Standard - students implemented an applied research project to address an organizational or societal problem, written a formal report of findings and recommendations, and produced a reflection of their experiences and its implications for their future. In the case of a prototype-based project, the student implemented the prototype to meet the specifications determined in the previous two courses in the sequence. While the project topics had a wide variety, students designs incorporate comprehensive cybersecurity principles, resulting in secure systems that are resilient against breaches. There is a clear and thorough application of cybersecurity best practices, demonstrating a strong understanding of how to safeguard intellectual property.

CYBR-5961 - 21 - 5 students * Master Research Prospectus - 100% Meet Standard - All students identified the purpose and scope of the problem they intend to address. This is the first of a 3-sequence course. Students choose a topic to apply cybersecurity best practices to safeguard intellectual property.

CYBR-5963 - 21 - 8 students * Master Research Project - 100% Meet Standard - students implemented an applied research project to address an organizational or societal problem, written a formal report of findings and recommendations, and produced a reflection of their experiences and its implications for their future. In the case of a prototype-based project, the student implemented the prototype to meet the specifications determined in the previous two courses in the sequence. While the project topics had a wide variety, students designs incorporate comprehensive cybersecurity principles, resulting in secure systems that are resilient against breaches. There is a clear and thorough application of cybersecurity best practices, demonstrating a strong understanding of how to safeguard intellectual property.

Summer 2022

CYBR-5961 -11 - 2 students* Master Research Project - 100% Meet Standard - All students identified the purpose and scope of the problem they intend to address. This is the first of a 3-sequence course. Students choose a topic to apply cybersecurity best practices to safeguard intellectual property.

Fall 2022

CYBR-5963- 21 - 4 students * Master Research Project - 100% Meet Standard students implemented an applied research project to address an organizational or societal problem, written a formal report of findings and recommendations, and produced a reflection of their experiences and its implications for their future. In the case of a prototype-based project, the student implemented the prototype to meet the specifications determined in the previous two courses in the sequence. While the project topics had a wide variety, students designs incorporate comprehensive cybersecurity principles, resulting in secure systems that are resilient against breaches. There is a clear and thorough application of cybersecurity best practices, demonstrating a strong understanding of how to safeguard intellectual property.

CYBR-5962 - 11 - 1 students * Master Research Prospectus - 100% Meet Standard students created an applied research design that includes a proposal demonstrating a strong understanding of how to safeguard intellectual property for addressing the organizational problem that was identified and described in CYBR 5961.

CYBR-5962 - 21 - 2 students * Master Research Prospectus - 100% Meet Standard students created an applied research design that includes a proposal demonstrating a strong understanding of how to safeguard intellectual property for addressing the organizational problem that was identified and described in CYBR 5961.

SLO 4: Graduates will be able to apply information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

CYBR 5010, Networking Concepts

Spring 2023

CYBR-5010 -12 - 13 students * Final Project 85% Meet Standard and 15% Approaches Standard. Students who did not meet the standards withdrew the course. Students who meet the standard The final project evaluates the criteria as follows students are given a role-play case scenario as a Network Architect who needs to perform a security assessment on the network and design a solution to make a company's network more secure at every layer. Students who met the standard were able to assess and build

a secured network Students utilized information security principles learned in CYBR-5000 and CYBR-5010 and exhibited a deep understanding of information security principles and applied them consistently to safeguard systems from threats..Students analyzed detection mechanisms, and mitigation strategies as part of this final project, which shows an understanding of information security principles and applies them consistently to safeguard systems from threats. Students who did not perform well did not complete all the requirements for the final project.

CYBR-5010 -13 - 14 students ** Final Project- 100% Meet Standard Students who did not meet the standards withdrew the course. Students who meet the standard The final project evaluates the criteria as follows students are given a role-play case scenario as a Network Architect who needs to perform a security assessment on the network and design a solution to make a company's network more secure at every layer. Students who met the standard were able to assess and build a secured network Students utilized information security principles learned in CYBR-5000 and CYBR-5010 and exhibited a deep understanding of information security principles and applied them consistently to safeguard systems from threats..Students analyzed detection mechanisms, and mitigation strategies as part of this final project, which shows an understanding of information security principles and applies them consistently to safeguard systems from threats.
CYBR-5010 -14 - 10 students ** Final Project 91% Meet Standard and 9% Approaches Standard. Students who did not meet the standards withdrew the course. Students who meet the standard The final project evaluates the criteria as follows students are given a role-play case scenario as a Network Architect who needs to perform a security assessment on the network and design a solution to make a company's network more secure at every layer. Students who met the standard were able to assess and build a secured network Students utilized information security principles learned in CYBR-5000 and CYBR-5010 and exhibited a deep understanding of information security principles and applied them consistently to safeguard systems from threats..Students analyzed detection mechanisms, and mitigation strategies as part of this final project, which shows an understanding of information security principles and applies them consistently to safeguard systems from threats. Students who did not perform well did not complete all the requirements for the final project.

CYBR-5010 -15 - 9 students ** Final Project 100% Meet Standard All students achieved the standard during the final project evaluates the criteria as follows students are given a role-play case scenario as a Network Architect who needs to perform a security assessment on the network and design a solution to make a company's network more secure at every layer. Students who met the standard were able to assess and build a secured network Students utilized information security principles learned in CYBR-5000 and CYBR-5010 and exhibited a deep understanding of information security principles and applied them consistently to safeguard systems from threats..Students analyzed detection mechanisms, and mitigation strategies as part of this final project, which shows an understanding of information security principles and applies them consistently to safeguard systems from threats. Students who did not perform well did not complete all the requirements for the final project.

CYBR 5020, Data Administration
Spring 2023
CYBR-5020 - 11- 2 students * Final Project 100% Meet Standard All students were able to meet the standard in the Final Project students are asked in a case scenario to propose a company which is currently a non-health care company, but the CEO what technical challenges are present as he is pivoting into the health care sector (and the company would be handling ePHI). Students were able to apply cybersecurity principles to analyze, detect and mitigate vulnerabilities and intrusions proposing a plan to protect the infrastructure and data.

CYBR 5030, Cyber Threats
Spring 2023
CYBR-5030 - 21 - 18 students * Final Project 100% Meet Standard During the final project, students act as the newly hired CIO/CISO in an organization that has PCI requirements, a third party vendor to conduct an internal and external pen test per PCI requirements. 100% of the students utilized the PenTest Execution Standard (PTES) for reporting. Students were involved in the pen test as an active stakeholder where they were able to discover and mitigate vulnerabilities. As part of this report, students met the standard by reporting on existing network traffic controls,network ranges owned by the organization, and identified possible weaknesses determining the impact of a security breach on confidentiality of the company’s information and Internal infrastructure and availability.

CYBR-5030 - 22 - 17 students * Final Project 100% Meet Standard During the final project, students act as the newly hired CIO/CISO in an organization that has PCI requirements, a third party vendor to conduct an internal and external pen test per PCI requirements. 100% of the students utilized the PenTest Execution Standard (PTES) for reporting. Students were involved in the pen test as an active stakeholder where they were able to discover and mitigate vulnerabilities. As part of this report, students met the standard by reporting on existing network traffic controls,network ranges owned by the organization, and identified possible weaknesses determining the impact of a security breach on confidentiality of the company’s information and Internal infrastructure and availability.

CYBR-5030 - 23 - 13 student * Final Project 87% Meet Standard - 13% Do not Meet Standard. During the final project, students act as the newly hired CIO/CISO in an organization that has PCI requirements, a third party vendor to conduct an internal and external pen test per PCI requirements. 100% of the students utilized the PenTest Execution Standard (PTES) for reporting. Students were involved in the pen test as an active stakeholder where they were able to discover and mitigate vulnerabilities. As part of this report, students met the standard by reporting on existing network traffic controls,network ranges owned by the organization, and identified possible weaknesses determining the impact of a security breach on confidentiality of the company's information and Internal infrastructure and availability.

CYBR 5230, Intrusion Detection and Analysis

Spring 2023

CYBR-5230- 21 - 6 students * Final Project - 86% Meet Standard - 14% Do not Meet Standard. Students who did not meet the standards withdrew the course. Students who meet the standard. In the final paper,students who met the standard combined Proactive efforts to decrease risk and improve security, Reactive threat detection effort, details on how to analyze intrusions in your environment and a summary of other aspects across a cybersecurity organization that relate to intrusion detection and analysis, but were not covered in depth in this course (XDR, SIEM, etc.)

CYBR-5230- 22 - 8 students ** Final Project 89% Meet Standard - 11% Do not Meet Standard Students who did not meet the standards withdrew the course. Students who meet the standard. In the final paper,students who met the standard combined Proactive efforts to decrease risk and improve security, Reactive threat detection effort, details on how to analyze intrusions in your environment and a summary of other aspects across a cybersecurity organization that relate to intrusion detection and analysis, but were not covered in depth in this course (XDR, SIEM, etc.)

CYBR-5230- 23 - 10 students ** Final Project 100% Meet Standard In the final paper,students who met the standard combined Proactive efforts to decrease risk and improve security, Reactive threat detection effort, details on how to analyze intrusions in your environment and a summary of other aspects across a cybersecurity organization that relate to intrusion detection and analysis, but were not covered in depth in this course (XDR, SIEM, etc.)

CYBR-5230- 24 - 8 students ** Final Project 88% Meet Standard - 13% Approaches Standard Students who did not meet the standards withdrew the course. Students who meet the standard. In the final paper,students who met the standard combined Proactive efforts to decrease risk and improve security, Reactive threat detection effort, details on how to analyze intrusions in your environment and a summary of other aspects across a cybersecurity organization that relate to intrusion detection and analysis, but were not covered in depth in this course (XDR, SIEM, etc.)

CYBR-5230- 25 - 11 students ** Final Project 82% Meet Standard - 18% Approaches Standard Students who did not meet the standards withdrew the course. Students who meet the standard. In the final paper,students who met the standard combined Proactive efforts to decrease risk and improve security, Reactive threat detection effort, details on how to analyze intrusions in your environment and a summary of other aspects across a cybersecurity organization that relate to intrusion detection and analysis, but were not covered in depth in this course (XDR, SIEM, etc.)

CYBR 5240, Cloud Security

Summer 2022

CYBR-5240- 11 - 4 students * Final Project 100% Meet Standard

Students worked individually to demonstrate their knowledge of Cloud Security by applying the concepts and theories to create a Final Paper. Students sucessfully Described the processes and reference NIST Frameworks to ensure Cloud Computing Security efforts capitalize on lasting security value to the institution. Students addressed using Cybersecurity Principles how to analyze, detect, and mitigate vulnerabilities in the Cloud. Also students created a SWOT analysis to compare the different cloud provider solutions studied in this course: GCP, AWS and Azure.

CYBR 5961/ CYBR 5262/ CYBR 5963 -Master Research Project I/II/III

Spring 2023

CYBR-5961 - 11 - 1 students * Master Research Prospectus - 100% Meet Standard - All students identified the purpose and scope of the problem they intend to address . Students include a section for background information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

CYBR-5963 - 11 - 9 students * Master Research Project - 100% Meet Standard - students implemented an applied research project to address an organizational or societal problem, written a formal report of findings and recommendations, and produced a reflection of their experiences and its implications for their future. In the case of a prototype-based project, the student

implemented the prototype to meet the specifications determined in the previous two courses in the sequence. While the project topics had a wide variety, students designs incorporate information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

CYBR-5961 - 21 - 5 students * Master Research Prospectus - 100% Meet Standard - All students identified the purpose and scope of the problem they intend to address. Students include a section for background information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

CYBR-5963 - 21 - 8 students * Master Research Project - 100% Meet Standard - students implemented an applied research project to address an organizational or societal problem, written a formal report of findings and recommendations, and produced a reflection of their experiences and its implications for their future. In the case of a prototype-based project, the student implemented the prototype to meet the specifications determined in the previous two courses in the sequence. While the project topics had a wide variety, students designs incorporate information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

Summer 2022

CYBR-5961 -11 - 2 students* Master Research Project - 100% Meet Standard - All students identified the purpose and scope of the problem they intend to address. Students include a section for background information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

Fall 2022

CYBR-5963- 21 - 4 students * Master Research Project - 100% Meet Standard tudents implemented an applied research project to address an organizational or societal problem, written a formal report of findings and recommendations, and produced a reflection of their experiences and its implications for their future. In the case of a prototype-based project, the student implemented the prototype to meet the specifications determined in the previous two courses in the sequence. While the project topics had a wide variety, students designs incorporate information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

CYBR-5962 - 11 - 1 students * Master Research Prospectus - 100% Meet Standard students created an applied research design that includes a proposal for addressing the organizational problem that was identified and described in CYBR 5961 and include information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

CYBR-5962 - 21 - 2 students * Master Research Prospectus - 100% Meet Standard students created an applied research design that includes a proposal for addressing the organizational problem that was identified and described in CYBR 5961 and include information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

Attached is the Learning Outcome Rubric which is used by the faculty to assess the SLOs

5. Findings: Interpretations & Conclusions

What have you learned from these results? What does the data tell you?

General Conclusions: Our Cybersecuirty master's program grew exponentially. We offered multiple sections of certain courses to support the demand. This growth is associated with our programs open up to the international students market. This also presented some challenges because courses needed to be offered on campus for the first time due to immigration requirements to comply with the international students visa. Most of the students that approached the standard because they withdrew the course, stopped participating in the class (and thus did not submit the final assignment/artifact) or they did not submit the final assignment/artifact after completing other assignments in the course or they did not submit an assignment/artifact that fulfill the criteria to meet the standard. To put this in perspective, a total of 5 students across CYBR-5030-23, CYBR-5010-12, CYBR-5010-14 did not meet the standard due international students who transferred out to other universities for SLO 3. Also, a total of 4 students, across CYBR-5020-11 (3 students), and CYBR-5030-21 approached the standard for SLO 3. Of these 3 students, 1 of them failed to approach the standard because they did not submit the assignment/artifact and 3 of them did not submit an assignment/artifact that fulfilled the criteria to meet the standard. This means, then, that 3 % did not approach the standard while 94% met the standard, and 3% did not meet the standards. A total of 7 students across CYBR-5010-12, CYBR-5010-14, CYBR-5030-21, CYBR-5230-21, CYBR-5230-22 did not approach the standard for SLO 4. Of these 4 students, 2 failed to meet the standard because they did not submit the assignment/artifact and 2 did not submit an assignment/artifact that fulfilled the criteria to meet the standard, and 3 students got zero on the assignments due to academic integrity issues. Additionally, a total of 4 students across CYBR-5030-21, CYBR-5230-24, CYBR-5230-25 did not approach the standard for SLO 4.This means, then, that 4% did not meet the standard, while 2% approached the standard, and 94% met the standard. We have to consider why students violate academic integrity. Since Nov 2022 with the introduction of chatGPT, we saw an increase in plagiarism,collusion, and cheating. We change the assignments prompts. Also, we need to understand why some students are not fulfilling the criteria for the assignments or submitting the final assignments/artifacts. Our student population has changed from online domestic

students to domestic and international students. We still teach adult students but the majority of the students are full time international students while the domestic students work and family responsibilities. The modality of the classes changed too as we offered online and on-campus. Despite the changes, we still have cases of students that are "intimidated" by the final assignment. Actually, I believe this has increased since we now have students whose english is not the first language. Do we need to provide different explicit instructions for instance a video, written instructions in the assignments? Do students feel comfortable with the instructions? While I think it is good that 94% of students approached or met the standard for SLO 3 and SLO 4, I think more needs to be done to increase the percentage of students that meet the standard for each SLO.

SLO 3:

In the Summer 1 of 2022 section of CYBR 5961 (Master Research Project I), 100% of the students met the standard. In the Fall 2021 section of CYBR 5220-11 50% of the students, CYBR-5220-12 (Incident Response and Mitigation), 100% of the students and CYBR-5962-11 (Master Research Project) , 100% of the students met the standard. The concern here is CYBR-5220-11, this was an online class. Half of the students did not submit the assignments or were poorly done. This could be considered as difficulty managing time, life balance from some students. We also saw students having issues with completing hands-on activities and discussions due to the amount of time consumed to complete. The entire cohort of CYBR-5962-11 were adult students who were already working. They were able to get permission to address company issues in their master research projects. Students were able to use the knowledge based learned in the master program in proposing solutions for their company issues with the evidence-based approach. Projects type included: UX/UI design impact on phishing emails, threat analysis, cloud computing, among other topics.In Spring 1 2022, a section of CYBR-5020 100% met the standard. In the Spring 2 2022, we had our biggest cohort and had to offered four sections of CYBR-5010 (Networking Concepts), 0% of the students did not meet the standard, CYBR-5010-12, 15% approached the standard, CYBR-5010-14, 9% approached the standard, 85% and 9% met the standard for these sections. CYBR-5010-13 & 15 sections 100% of students met the standard. CYBR-5010 is the second course of the degree and in two sections students struggled with meeting deadlines due to misunderstanding in due dates for assignments from newly arrived students. While the student population is adults, due to the in-person courses are new for us and international students, first assignments need to be shifted and distributed so the first week of class students can adapt well to the course. This will also benefit domestic students. A section of CYBR-5963-11 was also offered during the Fall 2022, and 100% of the students met the standard. This continues being a highlight of our program students showcase their knowledge and skill sets learned in the program.In the Spring 1 2023 a section of CYBR 5961-21, CYBR-5962-21 and CYBR-5963-21 (Master Research Project I, II, and III) , 100% of the students met the standard. The master research project is a 3-course sequence. Once the students choose a project in Master Research Project I, they need to develop a proposal, prototype, write a paper, and present. Students were comfortable with their soft skills since they are already working, they have good communication skills. Master Research Projects were so well done that the students obtained jobs, got promotions, or recognition from their company mentors. A student in particular used the knowledge acquired in the master program to Assess Challenges for Threat Hunting in Cloud Environments. This showcases the implementation of network case studies in the cloud and incorporation of cloud data management systems to protect intellectual property using cybersecurity principles.

A total of 149 students enrolled in Cybersecurity courses, 140 (94%) meet the standard, 4 students (3%) approach standard and 5 students (3%) Do not meet standard. Overall during the 2022-23 Academic Year a 94 % of the students meet SLO3.

SLO 4

In the Summer 1 of 2022 section of CYBR 5961 (Master Research Project I) and CYBR-5240 (Cloud Security) had a 100% of the students met the standard. In the Fall 2021 section of CYBR-5962-11 (Master Research Project) , 100% of the students met the standard. The entire cohort of CYBR-5962-11 were adult students who were already working. They were able to get permission to address company issues in their master research projects. Students were able to use the knowledge based learned in the master program in proposing solutions for their company issues with the

evidence-based approach. Projects type included: UX/UI design impact on phishing emails, threat analysis, cloud computing, among other topics. Despite the variety of the topics, students exhibited a deep understanding of information security principles and applied them consistently to safeguard systems from threats. In the Spring 2 2022, we had our biggest cohort and had to offered four sections of CYBR-5010 (Networking Concepts), 0% of the students did not meet the standard, CYBR-5010-12, 15% approached the standard, CYBR-5010-14, 9% approached the standard, 85% and 9% met the standard for these sections. CYBR-5010-13 & 15 sections 100% of students met the standard. CYBR-5010 is the second course of the degree and in two sections students struggled with meeting deadlines due to misunderstanding in due dates for assignments from newly arrived students. While the student population is adults, due to the in-person courses are new for us and international students, first assignments need to be shifted and distributed so the first week of class students can adapt well to the course. This will also benefit domestic students. Students appreciate the hands-on activities especially involving networking,vulnerability analysis, detection, and mitigation. A section of CYBR-5963-11 was also offered during the Fall 2022, and 100% of the students met the standard. This continues being a highlight of our program students showcase their knowledge and skill sets learned in the program.In Spring 2 2023, the new cohort of international students took CYBR-5230, we offered 5 sections of this course, CYBR-5030-21 with a 86% meet the standard and 14% approach the standard, CYBR-5030-22 89% meet the standard and 11% approach the standard, CYBR-5230 100% student met the standard,CYBR-5230, 88% meet the standard and 12% approach the standard ,and CYBR-5230 82% meet the standard and 18% approach the standard. A total of 43 students took CYBR-5230. 38 students meet the standard while 5 students approach the standard. Out of these 5 students, they either failed the assignments due to a plagiarism issue or failing to analyze vulnerabilities. Since this is a more advanced course, perhaps it should be offered later on in the roadmap. Tnere are some courses of reviewing the Spring 1 2023 sections of CYBR 5961-21, CYBR-5962-21 and CYBR-5963-21 (Master Research Project I, II, and III) , 100% of the students met the standard. The master research project is a 3-course sequence. Once the students choose a project in Master Research Project I, they need to develop a proposal, prototype, write a paper, and present. Students were comfortable with their soft skills since they are already working, they have good communication skills. Master Research Projects were so well done that the students obtained jobs, got promotions, or recognition from their company mentors. A student in particular used the knowledge acquired in the master program to Assess Challenges for Threat Hunting in Cloud Environments. This student applied information security principles to analyze, detect and mitigate vulnerabilities and intrusions in Cloud Environment.

In summary, a total of 179 students enrolled in Cybersecurity courses, 168 students (94%) meet the standard, 4 students (3%) approach standard, and 5 students (3%) Do not meet standard. Overall during the 2022-23 Academic Year a 94 % of the students meet SLO4.

6. Closing the Loop: Dissemination and Use of Current Assessment Findings

A. When and how did your program faculty share and discuss these results and findings from this cycle of assessment?

The program director and faculty met at the end of Spring 2023 to discuss the results. We went through the data and discussed variables that might have impacted the data. We also discussed potential changes whether pedagogical or curricular. We discussed whether we needed a different artifact (e.g., an essay instead of an exam), whether we needed to change the expectations in our assignment prompts, or whether we needed to change our teaching techniques.

B. How specifically have you decided to use these findings to improve teaching and learning in your program? For example, perhaps you've initiated one or more of the following:

Changes to the Curriculum or Pedagogies	● Course content ● Teaching techniques ● Improvements in technology ● Prerequisites	● Course sequence ● New courses ● Deletion of courses ● Changes in frequency or scheduling of course offerings
Changes to the Assessment Plan	● Student learning outcomes ● Artifacts of student learning ● Evaluation process	● Evaluation tools (e.g., rubrics) ● Data collection methods ● Frequency of data collection

Please describe the actions you are taking as a result of these findings.

No changes to the assessment plan at this point. Based on student and faculty feedback, course frequency and scheduling are being revised to level the number of courses offered each term. Our program has tripled the size with 179 students taking SLO4 courses and 149 students taking SLO3 courses. We also added on-campus course modality due to immigration requirements associated with international students. This brought some challenges and some refinement to the way we manage course content. For instance, we utilized master templates to copied content to all sections in a course, but it was hard to make changes and push them to all sections. A new pilot way to handle multiple sections is to manage the Master Course templates using Canvas BluePrint, which allows to house content and share to any number of associated courses. Blueprint courses will be maintained by admins or course designers. Content added to the blueprint course will be synced to all associated courses, and content can be locked or unlocked for editing in the associated courses. For SLO 3, CYBR-5220 Incident Response and Mitigation, CYBR-5210 Networking concepts needs more clear instructions in the assignment/artifact to encourage students to complete assignments,participate in discussions, and commit deadlines. Slso more emphasis in incorporating (SLO3) data management and network systems to protect intellectual property using cybersecurity principles. For SLO 4 in CYBR-5030 (Cyber Threats) and CYBR 5230 (Intrusion Detection and Analysis) need more clear instructions in the assignment/artifacts. We feel that students need more instruction on this mode of writing, especially now that the majority of the population is non-native English speakers. We will work with the the Reinert Center for Transformative Teaching and Learning at SLU to support the students and faculty. We also have to work in assignment prompts especially in discussions since ChatGPT was released we have seen an increased in Academic Integrity Issues.

Due to the nature of Cybersecurity, books need to be updated in CYBR-5030, and 5210 to more current ones. .

If no changes are being made, please explain why.

7. Closing the Loop: Review of Previous Assessment Findings and Changes

A. What is at least one change your program has implemented in recent years as a result of assessment data?

From a previous assessment, changes were done to CYBR-5000 and 5220 to add more clear instructions. However, these courses are not part of SLO 3 and 4. Standardization of the Master Research Project options with their respective templates were used in SLO 3 & 4 successfully. All the Master research projects I,II and III have met 100% standard. . We continue hiring of new adjuncts and full time faculty since the program has grown exponentially, redesigning courses has begun according to the revised curriculum map.

B. How has this change/have these changes been assessed?

The Master Research projects have been evaluated by faculty mentors who work with students throughout the three-hour sequence. Students implemented an applied research project consistent with their approved project, wrote a formal report of findings and recommendations, and delivered a formal presentation summarizing the project. Every semester the university sends the blue evaluation for students to send evaluation of the courses more specifically, CYBR-5220 and CYBR-5220. Faculty sent a qualtric survey and met with the Director to review the courses.

C. What were the findings of the assessment?

Students who completed the three-hour sequence satisfactorily demonstrated the competencies gained during the MS Cybersecurity program. CYBR-5000 and CYBR-5220 have satisfactory reviews from students and faculty.

D. How do you plan to (continue to) use this information moving forward?

The four general Master Research Project options will continue to be offered to students. Courses will be redesigned according to what the assessments revealed.

IMPORTANT: Please submit any assessment tools (e.g., rubrics) with this report.

2021-2022 Assessment Data

Cybersecurity

SLO 1: Graduates will be able to apply program-specific knowledge to address practical problems using an ethical, evidence-based framework

		Fall 1 2021	Summer 1 2021	Summer 2 2021	Fall 2 2021	Fall 2 2021	Spring 2 2022	
		CYBR-5000-11	**CYBR-5961-11**	**CYBR-5961-21**	**CYBR-5962-21**	**CYBR-5963-21**	**CYBR-5963-21**	**TOTAL**
Does Not Meet Standard (0 to 69%)	**Unable to identify or apply relevant program-specific knowledge to practical problems. Solutions are incorrect, irrelevant, or demonstrate a fundamental misunderstanding of the problem context.**	0%	0%	0%	0%	0%	0%	0%
Approaches Standard (70 to 89%)	**Identifies and applies some relevant program-specific knowledge to practical problems, but inconsistencies are evident. Solutions are partially correct and address parts of the problem but may miss key aspects or lack depth.**	25%	0%	0%	0%	0%	0%	13%
Meets Standard (90 to 100%)	**Consistently identifies and accurately applies relevant program-specific knowledge to practical problems. Solutions are correct, comprehensive, and well-suited to the problem context, demonstrating a thorough understanding of the subject matter.**	75%	100%	100%	100%	100%	100%	87%
		Introduce	Evaluated	Evaluated	Evaluated	Evaluated	Evaluated	

2021-2022 Assessment Data

Cybersecurity

SLO 2: Graduates will be able to utilize argumentation skills appropriate for a given problem or context.

		Fall 1 2021	Fall 2 2021	Summer 1 2021	Spring 1 2022	Summer 1 2021	Summer 2 2021	Fall 2 2021	Spring 2 2022	
		CYBR 5000-11	**CYBR 5220-21**	**CYBR-5240-11**	**CYBR-5240-11**	**CYBR-5961-11**	**CYBR-5961-21**	**CYBR-5962-21**	**CYBR-5963-21**	**TOTAL**
Does Not Meet Standard (0 to 69	**Demonstrates a lack of understanding of argumentation skills, presenting arguments that are unclear, unsupported by evidence, or irrelevant to the problem or context. Arguments are often illogical or flawed, failing to address the issue effectively.**	0%	0%	0%	0%	0%	0%	0%	0%	0%
Approaches Standard (70 to 89%)	**Demonstrates basic argumentation skills, with arguments that are generally clear and relevant to the problem or context. Some evidence is used, but the connections between evidence and conclusions may be weak or underdeveloped. Arguments may lack depth or coherence, occasionally missing key aspects of the problem.**	25%	25%	0%	0%	0%	0%	0%	0%	10%
Meets Standard (90 to 100%)	**Effectively utilizes argumentation skills, presenting well-structured arguments that are clear, relevant, and supported by appropriate evidence. The arguments are logical, coherent, and directly address the problem or context. The use of evidence is strong, with clear connections to conclusions, demonstrating a thorough understanding of effective argumentation.**	75%	75%	100%	100%	100%	100%	100%	100%	90%
		Introduced	Reinforce	Reinforce	Reinforce	Evaluated	Evaluated	Evaluated	Evaluated	

SLO 1: Graduates will be able to apply program-specific knowledge to address practical problems using an e

	Fall 1 2021	Summer 1 2021	Summer 2 2021	Fall 2 2021	Fall 2 2021	Spring 2 2022
	CYBR-5000-11	**CYBR-5961-11**	**CYBR-5961-21**	**CYBR-5962-21**	**CYBR-5963-21**	**CYBR-5963-21**
1	M	M	M	M	M	M
2	A			M	M	M
3	M				M	M
4	M				M	
5	A					
6	M					
7	M					
8	M					
9	A					
10	M					
11	M					
12	M					
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						

D	0	0	0	0	0	0
A	3	0	0	0	0	0
M	9	1	1	2	4	3
TOTAL	12	1	1	2	4	3

D	0%	0%	0%	0%	0%	0%
A	25%	0%	0%	0%	0%	0%
M	75%	100%	100%	100%	100%	100%

ethical, evidence-based framework

Does Not Meet Standard (0 to 69%)
Approaches Standard (70 to 89%)
Meets Standard (90 to 100%)

Stopped participating in course
Did not submit final artifact
Never participated in course

0	**D**
3	**A**
20	**M**
23	**TOTAL**

0%	**D**
13%	**A**
87%	**M**

SLO 2: Graduates will be able to utilize argumentation skills appropriate for a given problem or context.

	Fall 1 2021	Fall 2 2021	Summer 1 2021	Spring 1 2022	Summer 1 2021	Summer 2 2021	Fall 2 2021	Fall 2 2021	Spring 2 2022
	CYBR 5000-11	**CYBR 5220-21**	**CYBR-5240-11**	**CYBR-5240-11**	**CYBR-5961-11**	**CYBR-5961-21**	**CYBR-5962-21**	**CYBR-5963-21**	**CYBR-5963-21**
1	M	M	M	M	M	M	M	M	M
2	A	M	M	M			M	M	M
3	M	A	M	M				M	M
4	M	M	M	M				M	
5	A		M	M					
6	M		M						
7	M		M						
8	M		M						
9	A								
10	M								
11	M								
12	M								
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									
24									
25									

D	0	0	0	0	0	0	0	0	0
A	3	1	0	0	0	0	0	0	0
M	9	3	8	5	1	1	2	4	3
TOTAL	12	4	8	5	1	1	2	4	3

D	0%	0%	0%	0%	0%	0%	0%	0%	0%
A	25%	25%	0%	0%	0%	0%	0%	0%	0%
M	75%	75%	100%	100%	100%	100%	100%	100%	100%

Does Not Meet Standard (0 to 69%)
Approaches Standard (70 to 89%)
Meets Standard (90 to 100%)

Stopped participating in course
Did not submit final artifact
Never participated in course

0	**D**
4	**A**
36	**M**
40	**TOTAL**

0%	**D**
10%	**A**
90%	**M**

Cybersecurity
Learning Outcomes Rubric

Learning Outcome	Does Not Meet Standard	Approaches Standard	Meets Standard
Graduates will be able to apply program-specific knowledge to address practical problems using an ethical, evidence-based framework.	Unable to identify or apply relevant program-specific knowledge to practical problems. Solutions are incorrect, irrelevant, or demonstrate a fundamental misunderstanding of the problem context.	Identifies and applies some relevant program-specific knowledge to practical problems, but inconsistencies are evident. Solutions are partially correct and address parts of the problem but may miss key aspects or lack depth.	Consistently identifies and accurately applies relevant program-specific knowledge to practical problems. Solutions are correct, comprehensive, and well-suited to the problem context, demonstrating a thorough understanding of the subject matter.
Graduates will be able to utilize argumentation skills appropriate for a given problem or context.	Demonstrates a lack of understanding of argumentation skills, presenting arguments that are unclear, unsupported by evidence, or irrelevant to the problem or context. Arguments are often illogical or flawed, failing to address the issue effectively.	Demonstrates basic argumentation skills, with arguments that are generally clear and relevant to the problem or context. Some evidence is used, but the connections between evidence and conclusions may be weak or underdeveloped. Arguments may lack depth or coherence, occasionally missing key aspects of the problem.	Effectively utilizes argumentation skills, presenting well-structured arguments that are clear, relevant, and supported by appropriate evidence. The arguments are logical, coherent, and directly address the problem or context. The use of evidence is strong, with clear connections to conclusions, demonstrating a thorough understanding of effective argumentation.
Graduates will be able to construct and implement networks and data management systems that protect intellectual property using cybersecurity principles.	Fails to construct or implement networks and data management systems that protect intellectual property. Designs lack fundamental cybersecurity principles, resulting in systems that are vulnerable to breaches. There is little to no evidence of understanding how to safeguard intellectual property	Constructs and implements basic networks and data management systems with some measures to protect intellectual property. While some cybersecurity principles are applied, the systems may have vulnerabilities and may not fully protect against potential threats. The implementation shows an understanding of cybersecurity principles	Effectively constructs and implements networks and data management systems that robustly protect intellectual property. The designs incorporate comprehensive cybersecurity principles, resulting in secure systems that are resilient against breaches. There is a clear and thorough application of cybersecurity best practices, demonstrating a strong understanding of

		but lacks thoroughness and robustness.	how to safeguard intellectual property.
Graduates will be able to apply information security principles to analyze, detect and mitigate vulnerabilities and intrusions.	Demonstrates an inability to effectively apply information security principles. Analyses are incomplete or incorrect, and detection of vulnerabilities and intrusions is frequently missed. Mitigation strategies are ineffective or absent, showing a fundamental lack of understanding of information security principles	Apply information security principles adequately. Analyses uncover some vulnerabilities and intrusions but may overlook critical issues. Detection mechanisms function to some extent, and mitigation strategies are occasionally effective. However, the overall approach is not comprehensive, potentially leaving some vulnerabilities unaddressed.	Proficiently utilizes information security principles to conduct thorough analysis, detection, and mitigation of vulnerabilities and intrusions. Analyses are detailed and precise, detection mechanisms are dependable and proactive, and mitigation strategies are strong and well-executed. The graduate exhibits a deep understanding of information security principles and applies them consistently to safeguard systems from threats.