WRIGHT STATE UNIVERSITY

Program Assessment Report (PAR)

Cyber Security (CYBS) Masters Degree

REPORT PREPARED by: Pei, Yong

ACADEMIC YEAR COVERED BY THIS REPORT: 2021-2022

I. PROGRAM LEARNING OUTCOMES

The M.S. degree in Cyber Security is designed for individuals who want to develop skills to identify and resolve cybersecurity threats. The degree is focused on developing knowledge and skill applicable to protecting computer systems and computer networks. The program strengths include a unique blend of faculty expertise, well-equipped computer science and engineering laboratory facilities, and a balance of theory, practice, hardware, and software. Wright State University has been designated as a National Center of Academic Excellence in Cyber Defense Education through academic year 2025 for the Master of Science in Cyber Security with Cyber Defense Concentration. Program Learning Outcomes Graduates of the Master's of Science program in Cyber Security will have 1. The ability to integrate and apply current computer science and engineering knowledge and techniques to solve challenging problems in cyber security 2. The ability to apply concepts of cyber security defense and to use and integrate modern cyber security tools to effectively protect information, communication and computing systems The program learning outcomes are further mapped into the following specific course learning outcomes • Demonstrate in-depth understanding on building customized tools for basic network-traffic analysis. • Demonstrate how to use basic statistical methods to define effective anomaly intrusion detection systems • Implement standards (DES, AES, RSA, and etc) to increase the security of target systems • Use many of the security tools collected in BackTrack Linux • Design security defenses

II. PROCEDURES USED FOR ASSESSMENT

A. Direct Assessment

(i) Assessment Schedule Completed Program Learning Outcome Data Collection Term Review Term 1. Problem solving Annual Fall 2020, Fall 2021 2. Cyber defense Annual Fall 2020, Fall 2021 (ii) Alignment of program learning outcome to course learning outcomes 1. Problem solving CEG 6430 Demonstrate in-depth understanding on building customized tools for basic network-traffic analysis. CEG 6430 Demonstrate how to use basic statistical methods to define effective anomaly intrusion detection systems. CEG 6750 Implement standards (DES, AES, RSA, and etc) to increase the security of target systems 2. Cyber defense CEG 6420 Use many of the security tools collected in BackTrack Linux CEG 6424 Design security defenses (iii) Course learning outcomes to assignment being collected and assessed CEG 6430 Demonstrate in-depth understanding on building customized tools for basic network-traffic analysis. Course projects CEG 6430 Demonstrate how to use basic statistical methods to define effective anomaly intrusion detection systems Course projects CEG 6750 Implement standards (DES, AES, RSA, and etc) to increase the security of target systems Course projects CEG 6420 Use many of the security tools collected in BackTrack Linux Course projects CEG 6424 Design security defenses Course projects (iv) Collection of student artifacts assessed Spring 2020 CEG 6750 Course project descriptions and grade distributions. Spring 2020 CEG 6424 Course project descriptions and grade distributions. Fall 2020 CEG 6420 Course project descriptions and grade distributions. Fall 2020 CEG 6430 Course project descriptions and grade distributions.

B. Scoring of Student Work

The program learning outcomes are mapped to specific learning outcomes of the program core courses. Core courses are those that are required as a part of each student's Program of Study (POS). Therefore, each program outcomes are measured at least once over the course of a student's POS. Learning outcomes are directly assessed by evaluating the student performance in corresponding project assignments and exams.

C. Indirect Assessment

The program educational outcomes were established with input from and review by the external advisory board (EAB). In addition, the advisory board has reviewed and expressed approval of all major program changes made in the last five years. The Department of Computer Science and Engineering external advisory board includes representatives of local, regional and other businesses that historically hire Department graduates, as well as successful alumni of our programs. The board meets each Fall and Spring semester to review program objectives, curriculum and program changes, and new programs and courses. They make both high-level strategic recommendations and specific course and curriculum suggestions to the program. "College of Engineering and Computer Science, Master of Science Assessment of Learning Outcomes During Exit Interview" surveys are used as additional measures for indirect assessment. Survey is instrumented to collect graduating student assessment of self-efficacy for the learning outcomes. For each outcome students are asked to rate their own level of ability/achievement.

III. ASSESSMENT RESULTS/INFORMATION:

CEG 6750 – Course project descriptions and grade distributions. CEG 6420 – Course project descriptions and grade distributions. CEG 6424 – Course project descriptions and grade distributions. CEG 6430 – Course project descriptions and grade distributions.

Course learning outcome achieved. No concern is raised. Course learning outcome achieved. No concern is raised. Course learning outcome achieved. No concern is raised. Course learning outcome achieved. No concern is raised.

Implement standards (DES, AES, RSA, and etc) to increase the security of target systems. Use many of the security tools collected in BackTrack Linux. Design security defenses Demonstrate in-depth understanding on building customized tools for basic network-traffic analysis. Demonstrate how to use basic statistical methods to define effective anomaly intrusion detection systems

IV. ACTIONS TO IMPROVE STUDENT LEARNING

The program institutes a formal assessment program involving the collection of students performance checkpoint data related to each educational outcome of the program. Data have been collected since Fall, 2018. A formal program assessment was conducted by the Graduate Studies Committee of the Department of Computer Science and Engineering in Fall 2020 and Fall 2021. This data and assessment results are shared through Pilot among the GSC faculty members and student advisors. The GSC faculty and student advisors review all program courses every three years to ensure that course pre-requisites are relevant, student learning objectives are accurate and sequential courses are aligned. In response to the continual program assessments, in the last five years the Graduate Studies Committee has enacted several significant changes to the program curriculum designed to increase flexibility and student retention, while maintaining program rigor. Among these changes The number of core courses in the program was increased from 3 to 4. The additional core course, Security Attacks and Defenses, is designed to ensure that every student meets program outcomes by providing a hands-on environment to engage in cyber security operations utilizing techniques learned in the other core courses. The number of allowed thesis hours was also increased from 6 to 9, aligning the program with other M.S. degrees in the Department and allowing more research depth for thesis-track students.

V. SUPPORTING DOCUMENTS

Additional documentation, when provided, is stored in the internal Academic Program Assessment of Student Learning SharePoint site.