This studio course teaches four basic hands-on cyber-defense skills: configuring a firewall, implementing a host-based intrusion detection software tool, using the Metasploit tool to do penetration testing, and implementing a network intrusion detection tool. The first cyber-defense skill is on configuring an ACL (Access Control List) firewall. This module provides the students with a practical exercise applying their analytical skills to properly configure the ACL of a firewall and to verify the correctness of their firewall configurations. Through this exercise, the students also learn firewall oriented network security policies. The second cyber-defense skill is on implementing a host-based intrusion detection software tool which can detect suspicious user sessions on a computer. This module provides the students with a practical exercise applying their programming skills to solve anomaly detection problems. The third cyber-defense skill is on using the Metasploit tool to do penetration testing. This module provides the students with a practical exercise applying their programming skills to do penetration testing. The fourth cyber-defense skill is on implementing a network intrusion detection software tool which can detect suspicious network flows. This module provides the students with a practical exercise applying their programming skills to solve signature-based intrusion detection problems.

Enforced Prerequisite at Enrollment: CYBER 100S and SRA 231
Malware analysis and analytics. Through this course, the students will learn classification and clustering. The course relies extensively on hands-on exercises to teach students how to address malware issues using analysis techniques such as reverse engineering and static program analysis, as well as defense methods. It then builds on this foundation by teaching students how to use analytic approaches such as automatic malware trace classification and clustering. The course relies extensively on hands-on laboratory activities to help students obtain practical experience in malware analysis and analytics. Through this course, the students will gain concrete understandings on principles and practices of malware analysis and defense.

**Enforced Prerequisite at Enrollment:** IST 242 and IST 261 and CYBER 262

**CYBER 366: Malware Analytics**

3 Credits

Malware Analytics is an intermediate course required for students who are majoring in Cybersecurity Analytics and Operations. It is a three-credit hands-on course that teaches principles and practice of malware detection, analysis, and defense. The course begins by introducing the foundations of malware, including history, vulnerability, types, analysis methods, and defenses. It then builds on this foundation by teaching students how to address malware issues using analysis techniques such as reverse engineering and static program analysis, as well as how to use analytic approaches such as automatic malware trace classification and clustering. The course relies extensively on hands-on laboratory activities to help students obtain practical experience in malware analysis and analytics. Through this course, the students will gain concrete understandings on principles and practices of malware analysis and defense.

**Enforced Prerequisite at Enrollment:** CYBER 342W and ENGL 202 and 7th semester standing.

**CYBER 399: Foreign Studies**

1-12 Credits/Maximum of 12

Courses offered in foreign countries by individual or group instruction.

International Cultures (IL)

**CYBER 440: Cybersecurity Capstone**

3 Credits

Cybersecurity Capstone is an advanced, culminating course for students who are majoring in Cybersecurity. This course provides the student with a practical exercise, designed by the instructor. The initial weeks of the semester provide the student with an overview of several analytic frameworks that are used in cybersecurity shops and organizations. Then, the student reviews specific technical analysis methods in malware, static and dynamic analysis, file system exploration, security log file analysis and network analysis. The findings from these analyses are then integrated into the analytic framework, gaps are identified, further analysis is conducted to fill the gaps. In the final weeks of the semester, students construct a high level briefing that supplies appropriate levels of technical detail to top level executives.

**Enforced Prerequisite at Enrollment:** CYBER 342W and ENGL 202 and 7th semester standing.

**CYBER 494: Research Project**

1-12 Credits/Maximum of 12

Supervised student activities on research projects identified on an individual or small-group basis.

**CYBER 496: Independent Studies**

1-18 Credits/Maximum of 18

Creative projects, including research and design, that are supervised on an individual basis and that fall outside the scope of formal courses.

**CYBER 497: Special Topics**

1-9 Credits/Maximum of 9

Formal courses offered infrequently to explore, in depth, a comparatively narrow subject which may be topical or of special interest.

**CYBER 499: Foreign Studies**

1-12 Credits/Maximum of 12

Courses offered in foreign countries by individual or group instruction.

International Cultures (IL)