This 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 or CYBER 100) and IST 140

- **CYBER 294: Research Project**
  - 1-12 Credits/Maximum of 12
  - Supervised student activities on research projects identified on an individual or small-group basis.

- **CYBER 296: 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 297: 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 299: Foreign Studies**
  - 1-12 Credits/Maximum of 12
  - Courses offered in foreign countries by individual or group instruction.
  - International Cultures (IL)

- **CYBER 342W: Cyber Incident Handling and Response**
  - 3 Credits
  - Cyber Incident Handling and Response is an intermediate course appropriate for students who are majoring in Cybersecurity. This course provides the student with the background, experience and perspective that is required to document organizational preparation for cyber incidents, document cyber incident impact and resolution, document response strategies, as well as integrate business continuity planning into the organization. This is a writing intensive course, which requires each student to individually document cyber security incidents and communicate the impact of those incidents to the organization. Peer writing evaluation will help students to consider how effective their written communication skills are. Team writing assignments will provide students with the real-world experience of writing portions of organizational documents such as preparedness documentation, documenting the organization of computer incident response teams, documenting organizational disaster recovery plans, and documenting post-incident recovery plans. Students will receive peer feedback on their writing assignments, as well as direct feedback from the instructor with a goal of improving writing skills and conforming their writing styles to the expectations of organizations and industry.
Malware analysis and analytics. Through this course, the students will obtain hands-on experience in malware 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 262 and SRA 231 and SRA 236

**Writing Across the Curriculum**

**CYBER 362: Cybersecurity Analytics Studio**

3 Credits

Cyberattacks involve advanced and sophisticated techniques to infiltrate corporate computers, networks and enterprise systems and critical infrastructures. Types of attacks include advanced malware, zero day attacks and advanced persistent threats. Advance warning about attackers and intelligence about the threat landscape is considered by many security leaders to be essential features in cyber-defense. The massive increase in the rate of novel cyberattacks has made data-mining-based analytics techniques a critical component in detecting security threats. Big data analytics in security involves the ability to gather massive amounts of digital information to analyze, visualize and draw insights that can make it possible to predict and stop cyberattacks. This studio course teaches fundamental data-driven cybersecurity analytics skills using programming skills acquired in earlier courses. The course will be divided into three modules. The first module prepares students for security analytics, by refreshing or making them familiar with two popular data analytics programming languages (e.g., R and Python). The second module focuses on understanding the key cybersecurity analytics process including data exploration, data visualization and data preparation and examining popular data mining algorithms such as linear and logistic regression, decision trees, support vector machine, and neural networks and similar techniques for security analytics. In the third module, students use analytics process and methods for selected cybersecurity problems, such as security breaches, ZeroAccess Infection, Log Analytics, Access Analytics and Web Hacking Analytics. Through this studio course, the students will gain concrete understanding of security analytics processes, methodologies and how to apply these concepts and tools to real-world cybersecurity. A major component of the course will be several hands-on exercises and a final team-based project. Hands-on exercises provide students with knowledge, skills and hands-on experience of learning security analytics process and methodologies to address security problems. The team-based project allows students to apply what they have learned to address real world security threat. This course will incorporate collaborative and action-learning experiences wherever appropriate. Emphasis will be placed on developing and practicing writing and speaking skills through application of the concepts, theories and technologies that define the course.

**Enforced Prerequisite at Enrollment:** STAT 200 and IST 261 and CYBER 262 and enforced co-requisite SRA 365.

**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