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.
Malware analysis and analytics. Through this course, the students will
acquire hands-on laboratory activities to help students obtain practical experience in
classification and clustering. The course relies extensively on hands-on methods, and defenses. It then builds on this foundation by teaching
theoretical foundations of malware, including history, vulnerability, types, analysis
methods, and defenses. 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,
and concrete understandings on principles and practices of malware
analysis and defense.

**Enforced Prerequisite at Enrollment:** CYBER 262 and SRA 221 and
SRA 231

**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
then obtain experience in 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

**Enforced Prerequisite at Enrollment:** CYBER 342W and (ENGL 202A or
ENGL 202B or ENGL 202C or ENGL 202D) 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)