The Cyber Security concentration involves detecting, reporting, and responding to cyber threats, making encryption codes to securely pass information between systems, and taking appropriate measures to ensure the security of valuable information. Students will learn about server and network security, incident response and contingency planning, conducting vulnerability assessments, and penetration testing. Students who complete this new concentration will have the National Security Agency (NSA) and Department of Homeland Security (DHS) National Center of Academic Excellence in Cyber Defense Education (CAE-CDE) designation noted on their academic transcripts.

Area I: IT Upper-Level Core Curriculum (Required): 21 hours

- ITEC 3155 - Systems Analysis and Design
- ITEC 3235 - Human Computer Interaction
- ITEC 3245 - Database Principles
- ITEC 3300 - Project Management
- ITEC 4200 - Foundations of Information Assurance
- ITEC 4205 - Legal and Ethical Issues
- ITEC 4750 - Senior Capstone

Area II: IT Upper-Level Courses (Required): 27 hours

- ITEC 4345 - Cyber Systems Security
- ITEC 4344 - Ethical Hacking
- ITEC 4321 - Digital Forensics/Data Recovery
- ITEC 4341 - Incident Response/Cont. Plan
- ITEC 4361 - Software Security
- ITEC 4370 - Virtual Computing
- ITEC 4421 - Network Security
- ITEC 3328 - Linux Systems Admin
- ITEC 3325 - Windows Systems Admin

Area III: Additional Courses (Required): 12 hours

These courses may be taken in:

- Upper-level ITEC courses in the program;
- Informatics courses deemed appropriate for providing students with a strong foundation in IT as well as a deeper understanding or another discipline; or
- Approved transfer courses
Current Program:

Area I: IT Upper-Level Core Curriculum (Required): 21 hours
- ITEC 3155 - Systems Analysis and Design
- ITEC 3235 - Human Computer Interaction
- ITEC 3245 - Database Principles
- ITEC 3300 - Project Management
- ITEC 4200 - Foundations of Information Assurance
- ITEC 4205 - Legal and Ethical Issues
- ITEC 4750 - Senior Capstone

Area II: IT Upper-Level Courses (Required): 21 hours
Required (15 hours)
- ITEC 4421 - Network Security
- ITEC 4341 - Incident Response and Contingency Planning
- ITEC 4361 - Software Security
- C 4345 - Cyber Systems Security
- ITEC 4344 - Ethical Hacking

Select two (2) from the following (6 hours)
- ITEC 4321 Forensics/Data Recovery
- ITEC 4370 Virtual Computing
- ITEC 4299 Special Topics in Cybersecurity

Area III: Additional Courses (Required): 18 hours
These courses may be taken in:
- Upper-level ITEC courses in the program;
- Informatics courses deemed appropriate for providing students with a strong foundation in IT as well as a deeper understanding or another discipline; or
- Approved transfer courses

Modified Program:

Area I: IT Upper-Level Core Curriculum (Required): 21 hours
- ITEC 3155 - Systems Analysis and Design
- ITEC 3235 - Human Computer Interaction
- ITEC 3245 - Database Principles
- ITEC 3300 - Project Management
- ITEC 4200 - Foundations of Information Assurance
- ITEC 4205 - Legal and Ethical Issues
- ITEC 4750 - Senior Capstone

Area II: IT Upper-Level Courses (Required): 27 hours
- ITEC 4345 - Cyber Systems Security
- ITEC 4344 - Ethical Hacking
- ITEC 4321 - Digital Forensics/Data Recovery
- ITEC 4341 - Incident Response/Cont. Plan
- ITEC 4361 - Software Security
- ITEC 4370 - Virtual Computing
- ITEC 4421 - Network Security
- ITEC 3328 - Linux Systems Admin
- ITEC 3325 - Windows Systems Admin

Area III: Additional Courses (Required): 12 hours
These courses may be taken in:
- Upper-level ITEC courses in the program;
- Informatics courses deemed appropriate for providing students with a strong foundation in IT as well as a deeper understanding or another discipline; or
- Approved transfer courses
Middle Georgia State University has been designated as a National Center of Academic Excellence in Cyber Defense Education by NSA/DSH through the academic year 2022. This alignment meets the national certificate we received and will allow us to keep the designation after 2022.