CYBERSECURITY (CYBR)

CYBR C101 3 Units (54 lecture hours; 14 lab hours)
Introduction to Cybersecurity
Advisory: CST C104 or CIS C111.

Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

This course introduces the foundational concepts of cybersecurity, including social engineering, cybersecurity resilience, and cyber threats. The principles and structure of confidentiality, integrity, and availability are surveyed to provide a foundation for further study of cybersecurity. This course covers data privacy and security, system security, and personal security factors to examine the nature and roles of organizational security policies and risk management processes. Suitable for majors and non-majors interested in cybersecurity tools, techniques, and practices. Security exercises help students develop skills to prepare for careers such as Information Security Analyst, Cyber Crime Analyst, and Incident and Intrusion Analyst. Graded or Pass/No Pass option.

CYBR C132 3 Units (54 lecture hours; 14 lab hours)
Introduction to Ethical Hacking
Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Formerly CST C232B. This course is an introduction to the ethical and legal issues pertaining to network and computer security testing. Students will explore an introduction to the hacking methodology and network penetration testing using industry-recognized tools. Hands-on assignments will be used to help students develop introductory technical skills relevant to entry-level cybersecurity professionals, including demonstration of tools that can be used to gain information about a computer network, web applications, and databases. This course is intended for students with computer experience and an interest in cyber defense for private organizations. Graded or Pass/No Pass option.

CYBR C150 3 Units (54 lecture hours; 14 lab hours)
Introduction to Digital Forensics
Advisory: CST C128 and CST C158 and CYBR C230.

Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Students will explore an introduction to digital forensics using open source applications. Topics covered include chain of custody, forensic acquisition of data, forensic evidence reporting, expert witness testimony, timeline analysis, and anti-forensic techniques. Hands-on assignments will be used to develop introductory technical skills relevant to entry-level cybersecurity professionals. This course is intended for students with computer experience and an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated. Graded or Pass/No Pass option. **C-ID:** ITIS 165.

CYBR C160 3 Units (54 lecture hours; 14 lab hours)
Introduction to Incident Response
Advisory: CST C128 and CST C158 and CYBR C230.

Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Students will explore an introduction to cyber incident response using industry-recognized tools. Topics covered include incident response case studies, incident response tools used in industry, advanced persistent threats, documentation and technical reporting, timeline analysis, case management, and hunting, gathering, and foraging for cyber threats. Hands-on assignments will be used to help students develop introductory technical skills relevant to entry-level cybersecurity professionals. This course is intended for students with computer experience and an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated. Graded or Pass/No Pass option.

CYBR C170 3 Units (54 lecture hours; 14 lab hours)
Cybercrime and CSIRT Coordination
Advisory: CST C128 and CST C158 and CYBR C230.

Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Students will explore an introduction to laws relevant to cybercrime and the roles of the Cyber Security Incident Response Team (CSIRT). Topics covered include international, federal, and state laws relevant to cybercrime, an overview of the U.S. court system and jurisdictions, CSIRT coordination within the team and with stakeholders internal to the organization, ethics pertaining to cyber professionals, project management, technical writing, countermeasures, and compliance. This course is intended for students with an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated. Graded or Pass/No Pass option.

CYBR C225 3 Units (54 lecture hours)
Cybersecurity Governance, Risk, and Compliance
Advisory: CYBR C230 and C260.

Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Students will explore an introduction to governance, risk, and compliance in cybersecurity. Topics covered include cybersecurity risk management, improving critical cybersecurity infrastructure, cybersecurity governance and audit frameworks, and internal audits. This course is intended for students with an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated. Graded or Pass/No Pass option.

CYBR C227 **3 Units (54 lecture hours)**
Cyber-Physical Security: Protecting Critical Infrastructure
Advisory: CYBR C225 and CST C230.

Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Students will explore an introduction to cyber-physical security using a risk-informed, all-hazards approach to safeguarding critical infrastructure in cyberspace that emphasizes protections for privacy and civil liberties, transparent and accessible security processes, and domestic and international partnerships that further collective action. Topics covered include an analysis of cyber threats and vulnerabilities to understand more fully the interdependency of infrastructure systems nationwide, and that cyber and physical security are interdependent as core aspects of corporate risk management strategies. This course is intended for students with an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated. Graded or Pass/No Pass option.

CYBR C230 **3 Units (54 lecture hours; 14 lab hours)**
Network Security (Security+)
Advisory: CYBR C101 and CST C128.

Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Formerly CYBR C130 / CST C230. This course introduces the concepts of enterprise security, network and application attacks, cybersecurity resilience, secure network designs, and incident response. The principles and structure of threats, attacks, and vulnerabilities are surveyed to provide a foundation for further study of cybersecurity. This course covers governance, risk, and compliance to examine the nature and roles of organizational security policies and risk management processes. Hands-on exercises help students develop skills to prepare for careers such as Security Administrator or Systems Administrator. Preparation for the CompTIA Security+ certification exam. Graded or Pass/No Pass option.

CYBR C234 **3 Units (54 lecture hours; 14 lab hours)**
Web Application Security
Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Formerly CST C234. This course introduces the concepts of the Open Web Application Security Project (OWASP) top 10 vulnerabilities for websites and web applications. A survey of secure configurations and software development pertaining to web servers and web applications provides students with the fundamental information needed to protect systems against cyberattacks. Hands-on exercises using industry-recognized tools for application security audit and assessment help students develop skills to prepare for careers as an Application Security Architect or Software Engineer. Graded or Pass/No Pass option.

CYBR C242 **3 Units (54 lecture hours; 18 lab hours)**
Vulnerability Assessment (PenTest+)
Advisory: CST C128 or CST C201D and CYBR C230 and CYBR C132.

Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Formerly CST C242. This course introduces the concepts of planning and scoping assessments, legal and compliance requirements, vulnerability scanning, and penetration testing using industry-recognized tools and techniques. Students will learn how to develop a written report that contains proposed remediation techniques and provides practical recommendations that can be effectively communicated to management. Hands-on exercises will help students develop technical skills to prepare for careers such as Vulnerability Tester and Network Security Operations. Preparation for the CompTIA PenTest+ certification exam. Graded or Pass/No Pass option.

CYBR C250 **3 Units (54 lecture hours; 14 lab hours)**
Intermediate Digital Forensics
Advisory: CST C128 and CST C158 and CST C230.

Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Students will explore digital forensic techniques using industry-recognized tools. Topics covered include an introduction to network forensics and mobile device forensics, investigative and extraction tools, live acquisition data, evidence reporting, time-stomping and anti-forensic techniques, and the significance of time zones for forensic case analysis. Hands-on assignments will be used to develop technical skills relevant to entry-level cybersecurity professionals. This course is intended for students with computer experience and an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated. Graded or Pass/No Pass option.

CYBR C255 **3 Units (54 lecture hours; 18 lab hours)**
Cybersecurity Analyst (CySA+)
Advisory: CST C104 and CYBR C230 and CYBR C132.

Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Formerly CST C255 / CST C255B. This course emphasizes the protection of critical industry infrastructure, including topics such as threat management, software and systems security, security operations monitoring, incident response, and compliance assessment tools. Through hands-on exercises, students will learn the practical application of intermediate-level security skills using various industry-recognized security tools. The course provides a hands-on focus on Information Technology (IT) security process and procedures to help students prepare for careers such as Security Engineer, Vulnerability Analyst, and Threat Intelligence Analyst. Graded or Pass/No Pass option.

CYBR C256 3 Units (54 lecture hours; 14 lab hours)
Mobile Device Forensics
Advisory: CST C158 and C230 and CYBR C150.

Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Students will explore mobile device forensic techniques using industry-recognized tools. Topics covered include an introduction to mobile forensics, investigative and extraction tools, cloud storage, device seizure, use of Faraday bags, and evidence reporting. Hands-on assignments will be used to develop technical skills relevant to entry-level cybersecurity professionals. This course is intended for students with computer experience and an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated. Graded or Pass/No Pass option.

CYBR C260 3 Units (54 lecture hours; 14 lab hours)
Intermediate Incident Response
Advisory: CST C128 and CST C158 and CYBR C230.

Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Students will explore incident response techniques using industry-recognized tools. Topics covered include planning and scoping a cyber incident, information gathering for vulnerability assessment, vulnerability scanning and summarization reporting, report writing and best practices, obfuscation techniques, forensic artifacts, social media forensics, memory forensics, ethics, and compliance issues. Hands-on assignments will be used to develop technical skills relevant to entry-level cybersecurity professionals. This course is intended for students with computer experience and an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated. Graded or Pass/No Pass option.

CYBR C270 3 Units (54 lecture hours; 14 lab hours)
Certified Information Systems Security Professional
Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Formerly CST C260 / CST C260B. Students will explore the eight domains of information security known as the CISSP Common Body of Knowledge (CBK). Domain topics covered include security and risk management, asset security, security architecture and engineering, communications and network security, identity and access management, security assessment and testing, security operations, and software development security. Concepts covered will help students understand management level issues relevant to cybersecurity professionals, with roles such as IT Director/Manager, Security Systems Engineer, Security Analyst, Security Manager, Security Auditor, and Security Architect. Completing this course does not guarantee CISSP certification; however, the course addresses the exam objectives defined by (ISC)2 for the CISSP certification exam. This course is intended for students with computer experience and an interest in cyber defense for private organizations or government law enforcement. Graded or Pass/No Pass option.

CYBR C271 3 Units (54 lecture hours; 14 lab hours)
Become a Security Consultant
Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Formerly CST C271. This course introduces the concepts of professional security consulting for students with prior security training and work experience. Topics covered include types of security consulting, qualifications, setting up practice and finding clients, security tools and audits, and ethics for security consultants. The fundamentals of security consulting for private and government organizations are surveyed. Hands-on exercises using industry-recognized tools for security audit and assessment help students develop skills to prepare for a career as a Security Consultant. Graded or Pass/No Pass option.

CYBR C280 3 Units (54 lecture hours; 14 lab hours)
Advanced Digital Forensics & Incident Response Capstone
Advisory: CST C128 and CST C158 and CYBR C230.

Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Students will explore advanced digital forensics and incident response techniques using industry-recognized tools. Hands-on projects will be used to demonstrate technical skills relevant to entry-level cybersecurity professionals. Students will analyze a simulated case and report findings through technical documents and presentations. This course is intended for students with computer experience and an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated. Graded or Pass/No Pass option.

CYBR C291 3 Units (54 lecture hours; 14 lab hours)
CompTIA Advanced Security Practitioner
Grading Mode: Standard Letter, Pass/No Pass
Transfer Credit: CSU.

Formerly CST C231. This course emphasizes advanced security topics such as risk management, enterprise security architecture, enterprise security operations, technical integration of enterprise security. Through practice exercises, students will learn about the impact of industry trends on organizational security. The course focuses on Information Technology (IT) security process and procedures to help students prepare for careers including Security Architect, Application Security Engineer, and Technical Lead Analyst. Graded or Pass/No Pass option.