# CYBR C280: EMERGING TRENDS IN CYBERSECURITY

| Item | Value |
|---|---|
| Curriculum Committee Approval Date | 10/27/2023 |
| Top Code | 070800 - Computer Infrastructure and Support |
| Units | 3 Total Units |
| Hours | 68 Total Hours (Lecture Hours 54; Lab Hours 14) |
| Total Outside of Class Hours | 0 |
| Course Credit Status | Credit: Degree Applicable (D) |
| Material Fee | No |
| Basic Skills | Not Basic Skills (N) |
| Repeatable | No |
| Open Entry/Open Exit | No |
| Grading Policy | Standard Letter (S),<br>• Pass/No Pass (B) |

## Course Description

This course delves into the latest developments in the field of cybersecurity, equipping students with the knowledge and skills needed to protect against and respond to contemporary cybersecurity challenges. Students will explore emerging trends such as the following key areas: advanced threat landscape, cloud security, artificial intelligence and machine learning in cybersecurity, blockchain and cryptocurrency security, biometric and multifactor authentication, threat intelligence and information sharing, compliance and regulations, security automation and orchestration, emerging ethical and legal issues, future trends and predictive analysis, and case studies and practical applications. Hands-on projects will be used to demonstrate 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. ADVISORY: CYBR C150 and CYBR C160. Transfer Credit: CSU.

## Course Level Student Learning Outcome(s)

1. Given a simulated environment, demonstrate the appropriate use of tools to identify security gaps and develop a response plan.
2. Given a simulated case, analyze and organize digital evidence to produce a report of findings using appropriate, industry-recognized terminology.
3. Given a simulated environment, demonstrate the ability to locate indicators of compromise.

## Course Objectives

- 1. Explain the qualifications and certifications of the cybersecurity paths.
- 2. Explain the qualifications and certifications of the digital forensics career path.
- 3. Explain the technical skills needed for incident handling.
- 4. Outline law enforcement careers and emerging trends in the field of cybersecurity.
- 5. Demonstrate the techniques necessary to evaluate a case.
- 6. Discuss data breach case studies and other news articles related to cybersecurity incidents.

## Lecture Content

Project management and team coordination  Understanding formal reporting techniques  Forensics laboratories  National Forensics Lab Regional Computer Forensics Lab Timeline analysis  Using case management tools  Finding red team artifacts  Review case studies  Involving digital forensics Involving incident response scenarios Sandboxing and reverse-engineering  Gathering indicators of compromise

## Lab Content

Students will work with remote lab environments to complete hands-on activities. Identify cyberattack patterns Use timeline analysis tools Identify malware Identify pivot point of an attack Analyze the containment process Analyze the eradication process Analyze advanced persistent threats (APTs)

## Method(s) of Instruction

- Lecture (02)
- DE Live Online Lecture (02S)
- DE Online Lecture (02X)
- Lab (04)
- DE Live Online Lab (04S)
- DE Online Lab (04X)

## Instructional Techniques

This course will utilize a combination of lecture, hands-on guided laboratory assignments, classroom/discussion student interactions, problem solving, quizzes, tests, and troubleshooting assignments to achieve the goals and objectives of this course. All instructional methods are consistent across all modalities.

## Reading Assignments

Read about and research the role of the cybersecurity profession. Read about cybersecurity processes, procedures, and frameworks. Read about the cybersecurity maturity model certification and other compliance frameworks.

## Writing Assignments

Complete a report after examining and analyzing a simulated case or case studies.

## Out-of-class Assignments

Complete hands-on lab to evaluate, examine, and analyze a simulated case. Examine case studies related to cybersecurity incidents.

## Demonstration of Critical Thinking

Students will conduct technical analysis using best practices, processes, and procedures.

## Required Writing, Problem Solving, Skills Demonstration

Skills will be demonstrated through completion of hands-on lab exercises using forensics and incident handling tools and document the analysis performed in preparation for expert witness testimony.

## Eligible Disciplines

Computer information systems (computer network installation, microcomputer ...: Any bachelor's degree and two years of professional experience, or any associate degree and six years of professional experience. Computer service technology: Any bachelor's degree and two years of professional experience, or any associate degree and six years of professional experience.

## Other Resources

1. Coastline Library 2. Commonly referenced cybersecurity whitepapers and Open Educational Resources (OER), will be used along with the latest data breach case studies, such as: (ISC)2 https://www.isc2.org/ Verizon Data Breach Investigations Report (DBIR) https://www.verizon.com/business/resources/reports/dbir/ NIST Computer Security Resource Center Publications https://csrc.nist.gov/publications/cswp CrowdStrike Whitepapers https://www.crowdstrike.com/resources/white-papers/ SANS Information Security White Papers https://www.sans.org/white-papers/ MITRE - Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) https://www.mitre.org/