CYBR C160: INTRODUCTION TO INCIDENT RESPONSE

Item	Value
Curriculum Committee Approval Date	10/27/2023
Top Code	070800 - Computer Infrastructure and Support
Units	3 Total Units
Hours	72 Total Hours (Lecture Hours 54; Lab Hours 18)
Total Outside of Class Hours	0
Course Credit Status	Credit: Degree Applicable (D)
Material Fee	No
Basic Skills	Not Basic Skills (N)
Repeatable	No
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

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. ADVISORY: IT C128 and IT C158 and CYBR C230. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Identify common resolutions to basic cybersecurity incidents.
2. Given a case study, analyze to identify attack patterns based on the cyber kill chain process.
3. Demonstrate an understanding of the steps of the incident response process.

Course Objectives

- 1. Define cybersecurity incidents and their various forms, including breaches, malware attacks, and data leaks.
- 2. Describe the incident response process.
- 3. Identify the steps of the cyber kill chain process.
- 4. Describe the roles within a security incident response team and emerging industry trends.
- 5. Explain the role of incident response in reducing security risks and minimizing damage.
- 6. Explain how to identify strategies to contain and limit the impact of cybersecurity incidents.

Lecture Content

Incident Response Planning Preparation Identification Containment Eradication Recovery Lessons Learned Incident Response Detection and Decision Making Process and Procedures Intro to Timeline Analysis Threat Hunting Security Posture Advanced Persistent Threats (APT) Cyber Kill Chain Reconnaissance Weaponization Delivery Exploitation Installation Command and Control Actions on Objectives Hunting, Gathering, and Foraging Tools Documentation/Reporting Incident Response Recovery and Maintenance Incident Response Case Studies Incident Response Case Review (hands-on exercises)

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 Create a comprehensive report of the incident Analyze the containment process Analyze the eradication process Analyze advanced persistent threats (APTs) Create a comprehensive report of evidence collected

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

The major steps of the incident response process and procedures. The steps of incident response recovery and lessons learned. The cyber kill chain.

Writing Assignments

Document cyberattack patterns commonly found in enterprise settings. Document and summarize findings in a timeline analysis report.

Out-of-class Assignments

Analyze a simiulated cyber incident following incident response processes and procedures with tools communly used in industry. Analyze a simiulated cyber investigation to develop a timeline analysis report.

Demonstration of Critical Thinking

Students will conduct cyberattack 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 common detection tools and document analysis performed.

Eligible Disciplines

Computer information systems (computer network installation, microcomputer ...: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional

experience. Computer service technology: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional experience.

Textbooks Resources

1. Required Martinez, R.. Incident Response with Threat Intelligence: Practical insights into developing an incident response capability through intelligence-based threat hunting, ed. Packt Publishing, 2022

Other Resources

1. Coastline Library 2. OER - Open Educational Resources