CYBR C255: CYBERSECURITY ANALYST (CYSA+)

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
Open Entry/Open Exit	No
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

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. ADVISORY: IT C104 and CYBR C230. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Effectively analyze data from security monitoring activities and implement configuration changes to existing controls to improve security within software and networked systems.
2. Compare and contrast automation techniques and explain the application of proactive threat hunting.
3. Explain the importance of incident response processes and procedures and analyze potential indicators of compromise.
4. Use appropriate tools and methods to manage, prioritize, and respond to attacks and vulnerabilities.

Course Objectives

- 1. Describe the impact of malware and threats related to a given organizational infrastructure.
- 2. Explain how to perform incident response processes.
- 3. Demonstrate the use of threat-detection tools, perform data analysis, and interpret the results to secure an organization's applications and systems.
- 4. Outline the best practices of software and hardware assurance to secure an organization's infrastructure.
- 5. Define the process for analyzing data from security monitoring activities.
- 6. Specify potential indicators of compromise for network, host, and application-related incidents.
- 7. Share information about appropriate tools and methods to manage, prioritize, and respond to attacks and vulnerabilities.
- 8. Explain reporting and communication concepts related to vulnerability management and incident response activities.

Lecture Content

Threat and Vulnerability Management Explain the importance of threat data and intelligence Utilize threat intelligence to support organizational security Vulnerability management activities Output from common vulnerability assessment tools Threats and vulnerabilities associated with specialized technology Threats and vulnerabilities associated with operating in the cloud Controls to mitigate attacks and software vulnerabilities Software and System Security Security solutions for infrastructure management Best practices for software assurance Best practices for hardware assurance Security Operations and Monitoring Data from security monitoring activities Improve security through configuration changes to existing controls Proactive threat hunting Automation concepts and technologies Incident Response The incident response process Applying incident response procedures Analyzing indicators of compromise Basic digital forensics techniques Compliance and Assessment Data privacy and protection Security concepts supporting organizational risk mitigation Frameworks, policies, procedures, and controls

Lab Content

Perform vulnerability management activities Implement controls to mitigate attacks and vulnerabilities Apply security solutions for infrastructure management Implement configuration changes to improve security Apply incident response procedures Analyze potential indicators of compromise (IOCs) Utilize basic digital forensics techniques Identify and address vulnerabilities to suggest preventive measures

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 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 assigned chapters. Use online resources to research types of malware and cyberattacks.

Writing Assignments

Evaluate threat-detection tools. Evaluate threat-analysis tools. Report results.

Out-of-class Assignments

Perform data analysis on given attacks. Given a scenario interpret the results to identify vulnerabilities and risks to an organization.

Demonstration of Critical Thinking

Selection of the appropriate tool for specific test types to check the security of the network.

Required Writing, Problem Solving, Skills Demonstration

Included in reporting of insecure network infrastructure evaluation. Quizzes, discussion forums, and written assignments completed by students on a weekly basis.

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.

Textbooks Resources

1. Required Heath, M, Rogers, B., and Chapman, B. CompTIA CySA + Cybersecurity Analyst Certification All-in-One Exam Guide, 3rd ed. McGraw Hill, 2023

Other Resources

1. Coastline Library 2. IT white papers are available at no charge to all IT students through the Microsoft IT Academy website.