SPRINGFIELD TECHNICAL COMMUNITY COLLEGE

ACADEMIC AFFAIRS

Course Number: CSO-180 Class/Lect. Hours: 3 Lab Hours: 3 Credits: 4 Dept.: Electronics

Course Title: Cisco CCNA Cyber Security Operations Semester: Spring Year: 2019

Course Description, Prerequisite, Corequisite:

The Cisco CCNA Cyber Security Operations course is taught through the Cisco Networking Academy with the latest course material from Cisco. Cybersecurity operations jobs play a key part of securing information systems through the monitoring, detecting, investigating, analyzing, and responding to security events, thus protecting systems from cybersecurity risks, threats, and vulnerabilities. Such jobs are among the fastest-growing roles in IT, as organizations set up security operations centers (SOCs), and establish teams to monitor and respond to security incidents. Cybersecurity Operations course serves to prepare students for the world of working in a security operations center and provides the basis for building upon their future career goals in cybersecurity.

Prerequisite(s): CSO-155 and CSE-150 or permission from the instructor

OBJECTIVES/COMPETENCIES

Course Objectives	Competencies
Understand the role of the Cybersecurity Operations Analyst in the enterprise. Understand the fundamental theory of cybersecurity standards and practices. Understand/perform how to secure common desktop, server and network operating systems.	Explain the role of the Cybersecurity Operations Analyst in the enterprise. Explain why networks and data are attacked. Explain how to prepare for a career in Cybersecurity operations.

Course Objectives	Competencies
Understand common network protocols and infrastructure. Understand common cybersecurity attack vectors. Understand/perform current tactics for defending networks and systems from malicious attacks and malicious actors. Understand the common cryptographic fundamentals of networks and endpoint devices. Understand/Evaluate and Perform Security Monitoring of Networks and computer systems Understand/Evaluate and Perform Intrusions Data Analysis of Networks and computer systems Understand Indecent response and report handling	Explain and understand the concept of CIA (Confidentiality, Integrity, and Availability) Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses Explain the operation of the Windows Operating System. Explain how to secure Windows endpoints. Explain the features and characteristics of the Linux Operating System Perform basic operations in the Linux shell. Perform basic Linux administration tasks Analyze the operation of network protocols and services. Explain how the Ethernet and IP protocols support network communications and operations Explain how network services enable network functionality Explain network topologies and the operation of the network infrastructure. Explain how network devices enable wired and wireless network communication. Explain how devices and services are used to enhance network security Classify the various types of network attacks

Course Objectives	Competencies
	Explain how networks are attacked Explain the various types of threats and attacks. Use network monitoring tools to identify attacks against network protocols and services. Explain network traffic monitoring Explain how TCP/IP vulnerabilities enable network attacks Explain how common network applications and services are vulnerable to attack. Use various methods to prevent malicious access to computer networks, hosts, and data. Explain approaches to network security defense Use various intelligence sources to locate current security threats. Explain the impacts of cryptography on network security monitoring. Use tools to encrypt and decrypt data Explain how the public key infrastructure (PKI) supports network security. Explain endpoint vulnerabilities and attacks investigation process Use tools to generate a malware analysis report.

Course Objectives	Competencies
	Classify endpoint vulnerability assessment information Evaluate network security alerts Explain how security technologies affect security monitoring. Explain and Classify the types of log files used in security monitoring. Analyze network intrusion data to identify compromised hosts and vulnerabilities Explain how security-related data is collected Analyze intrusion data to determine the source of an attack. Explain how network security incidents are handled by CSIRTs. Apply incident response models, such as NIST 800-61r2 to a security incident. Use a set of logs to isolate threat actors and recommend an incident response plan.