Course Outcome Guide (COG)

Course:	CIS 245 CCNA Cybersecurity Operations	**Credits:**	3	**Instructor:**	Ken Quamme
Course Description:	CCNA Cybersecurity Operations v1.1 covers knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level Security Analyst working in a Security Operations Center (SOC).				

Concepts and Issues	Process Skills	Assessment Tasks	Intended Outcomes		
			Course	General Education or Program	Institutional
• Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events. • Explain the role of the Cybersecurity Operations Analyst in the enterprise. • Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses. • Explain the features and characteristics of the Linux Operating System. • Analyze the operation of network protocols and services. • Explain the operation of the network infrastructure.	• Evaluate cybersecurity operations and the risks in an industry sector • Use industry-standard models to explain security requirements in the cybersecurity operations. • Perform threat modeling activities to evaluate physical device security vulnerabilities in cybersecurity operations. • Explain the impact of emerging technologies on cybersecurity operations	• Documentation of tasks • Online tests and quizzes • Graded lab activities • Project-based final assessment • Final Assessment • Participation • Individual and group projects • Course Feedback	• Understand cybersecurity operations network principles, roles and responsibilities as well as the related technologies, tools, regulations and frameworks available. • Apply knowledge and skills to monitor, detect, investigate, analyze and respond to security incidents. • Apply for entry-level jobs as Assoicate Security Analyst and Incident Responder. • Take the Cisco Certified CyberOps Certification exam.	• Assemble a PC with components and install one or more operating systems resulting in a functioning PC. • Identify major network media types, including coaxial cable, UTP and fiber optic cable. • Design a small or medium sized computer network with media and configuring devices • Identify and secure PCs, servers, and networks	• Demonstrate effective communicatio n skills, and be able to use reasoning to analyze and solve problems.

• Classify the various types of network attacks. • Use network monitoring tools to identify attacks against network protocols and services. • Use various methods to prevent malicious access to computer networks, hosts, and data. • Explain the impacts of cryptography on network security monitoring. • Explain how to investigate endpoint vulnerabilities and attacks. • Evaluate network security alerts. • Analyze network intrusion data to identify compromised hosts and vulnerabilities. • Apply incident response models to manage network security incidents. • ASSESSMENT TASKS (FOR COURSE OUTCOMES)					