Course Outline

Information and Communication Technologies **REVISED June/2019**

Course Description:

This competency-based course is designed to prepare the student for the 210-255 SECOPS exam. The Implementing Cisco Cybersecurity Operations (SECOPS) exam (210-255) is a 90-minute, 60—70 question assessment. This is the second of two exams that must be passed to receive an associate-level CCNA Cyber Ops certification.

This course equips students with the basic knowledge, foundational principles, and entry-level skills to begin a career within a Security Operations Center (SOC), working with Cybersecurity Analysts at the associate level. The SECOPS exam tests a candidate's knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level Security Analyst working in a SOC.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

In addition, the United States Department of Defense (DoD) has approved Cisco CCNA Cyber Ops Certification for inclusion in the DoD 8570.01-M for the CCSP Analyst and CCSP Incident Responder categories.

The competencies in this course are aligned with the California High School Academic Content Standards and the California Career Technical Education Model Curriculum Standards.

Job Title: Information Security Analysts

Career Pathway: Networking

Industry Sector: Information and Communication Technologies

O*NET-SOC CODE: 15-1122.00

CBEDS Title: Network Security

CBEDS No.: 4646

77-65-80

Implementing Cybersecurity Operations

Credits: 5 **Hours:** 90

Prerequisites:
Enrollment requires completion of the Cybersecurity Operations Fundamentals (77-65-70) course and passing the CCNA Cyber Ops 210-250 SECFND Exam.

Recommended knowledge and skills:

Linux operating system
Mac OSX operating system
Microsoft Windows operating systems

NOTE: For Perkins purposes this course has been designated as both a **concentrator** and a **capstone** course.

This course **cannot** be repeated once a student receives a Certificate of Completion.

COURSE OUTLINE COMPETENCY-BASED COMPONENTS

A course outline reflects the essential intent and content of the course described. Acceptable course outlines have six components. (Education Code Section 52506). Course outlines for all apportionment classes, including those in jails, state hospitals, and convalescent hospitals, contain the six required elements:

(EC 52504; 5CCR 10508 [b]; Adult Education Handbook for California [1977], Section 100)

COURSE OUTLINE COMPONENTS **LOCATION**

GOALS AND PURPOSES Cover

The educational goals or purposes of every course are clearly stated and the class periods are devoted to instruction. The course should be broad enough in scope and should have sufficient educational worth to justify the expenditure of public funds.

The goals and purpose of a course are stated in the COURSE DESCRIPTION. Course descriptions state the major emphasis and content of a course, and are written to be understandable by a prospective student.

PERFORMANCE OBJECTIVES OR COMPETENCIES pp. 7-11

Objectives should be delineated and described in terms of measurable results for the student and include the possible ways in which the objectives contribute to the student's acquisition of skills and competencies.

Performance Objectives are sequentially listed in the COMPETENCY-BASED COMPONENTS section of the course outline. Competency Areas are units of instruction based on related competencies. Competency Statements are competency area goals that together define the framework and purpose of a course. Competencies fall on a continuum between goals and performance objectives and denote the outcome of instruction.

Competency-based instruction tells a student before instruction what skills or knowledge they will demonstrate after instruction. Competency-based education provides instruction which enables each student to attain individual goals as measured against pre-stated standards.

Competency-based instruction provides immediate and continual repetition and in competency-based education the curriculum, instruction, and assessment share common characteristics based on clearly stated competencies. Curriculum, instruction and assessment in competency-based education are: explicit, known, agreed upon, integrated, performance oriented, and adaptive.

COURSE OUTLINE COMPETENCY-BASED COMPONENTS (continued)

COURSE OUTLINE COMPONENTS **LOCATION**

INSTRUCTIONAL STRATEGIES p. 14

Instructional techniques or methods could include laboratory techniques, lecture method, small-group discussion, grouping plans, and other strategies used in the classroom.

Instructional strategies for this course are listed in the TEACHING STRATEGIES AND EVALUATION section of the course outline. Instructional strategies and activities for a course should be selected so that the overall teaching approach takes into account the instructional standards of a particular program, i.e., English as a Second Language, Programs for Adults with Disabilities.

UNITS OF STUDY, WITH APPROXIMATE HOURS ALLOTTED FOR EACH UNIT Cover

The approximate time devoted to each instructional unit within the course, as well as the total hours for the course, is indicated. The time in class is consistent with the needs of the student, and the length of the class should be that it ensures the student will learn at an optimum level. pp. 7-11

Units of study, with approximate hours allotted for each unit are listed in the COMPETENCY AREA STATEMENT(S) of the course outline. The total hours of the course, including work-based learning hours (community classroom and cooperative vocational education) is listed on the cover of every CBE course outline. Each Competency Area listed within a CBE outline is assigned hours of instruction per unit.

EVALUATION PROCEDURES p. 13

The evaluation describes measurable evaluation criteria clearly within the reach of the student. The evaluation indicates anticipated improvement in performances as well as anticipated skills and competencies to be achieved.

Evaluation procedures are detailed in the TEACHING STRATEGIES AND EVALUATION section of the course outline. Instructors monitor students' progress on a continuing basis, assessing students on attainment of objectives identified in the course outline through a variety of formal and informal tests (applied performance procedures, observations, and simulations), paper and pencil exams, and standardized tests.

REPETITION POLICY THAT PREVENTS PERPETUATION OF STUDENT ENROLLMENT Cover

After a student has completed all the objectives of the course, he or she should not be allowed to reenroll in the course. There is, therefore, a need for a statement about the conditions for possible repetition of a course to prevent perpetuation of students in a particular program for an indefinite period of time.

ACKNOWLEDGMENTS

Thanks to ROBERT YORGASON and ALEJANDRA SLACEDO for developing and editing this course outline. Acknowledgment is also given to ERICA ROSARIO for designing the original artwork for the course covers.

ANA MARTINEZ
Specialist
Career Technical Education

ROSARIO GALVAN
Administrator
Division of Adult and Career Education

APPROVED:

JOSEPH STARK
Executive Director
Division of Adult and Career Education

CALIFORNIA CAREER TECHNICAL EDUCATION MODEL CURRICULUM STANDARDS
Information and Communications Technologies Industry Sector
Knowledge and Performance Anchor Standards

1.0 Academics
Analyze and apply appropriate academic standards required for successful industry sector pathway completion leading to postsecondary education and employment. Refer to the Agriculture and Natural Resources academic alignment matrix for identification of standards

2.0 Communications
Acquire and accurately use Agriculture and Natural Resources sector terminology and protocols at the career and college readiness level for communicating effectively in oral, written, and multimedia formats.

3.0 Career Planning and Management
Integrate multiple sources of career information from diverse formats to make informed career decisions, solve problems, and manage personal career plans

4.0 Technology
Use existing and emerging technology to investigate, research, and produce products and services, including new information, as required in the Agriculture and Natural Resources sector workplace environment.

5.0 Problem Solving and Critical Thinking
Conduct short as well as more sustained research to create alternative solutions to answer a question or solve a problem unique to the Agriculture and Natural Resources sector, using critical and creative thinking, logical reasoning, analysis, inquiry, and problem-solving techniques.

.

6.0 Health and Safety
Demonstrate health and safety procedures, regulations, and personal health practices and determine the meaning of symbols, key terms, and domain-specific words and phrases as related to the Agriculture and Natural Resources sector workplace environment.

7.0 Responsibility and Flexibility
Initiate, and participate in, a range of collaborations demonstrating behaviors that reflect personal and professional responsibility, flexibility, and respect in the Agriculture and Natural Resources sector workplace environment and community settings.

8.0 Ethics and Legal Responsibilities
Practice professional, ethical, and legal behavior, responding thoughtfully to diverse perspectives and resolving contradictions when possible, consistent with applicable laws, regulations, and organizational norms.

9.0 Leadership and Teamwork
Work with peers to promote divergent and creative perspectives, effective leadership, group dynamics, team and individual decision making, benefits of workforce diversity, and conflict resolution as practiced in the Future Farmers of America (FFA) career technical student organization.

10.0 Technical Knowledge and Skills
Apply essential technical knowledge and skills common to all pathways in the Agriculture and Natural Resources sector, following procedures when carrying out experiments or performing technical tasks.

11.0 Demonstration and Application
Demonstrate and apply the knowledge and skills contained in the Agriculture and Natural Resources anchor standards, pathway standards, and performance indicators in classroom, laboratory, and workplace settings, and through the FFA career technical student organization.

B. Networking Pathway
Students in the Networking pathway prepare for careers that involve the implementation of computer services and software, support of multimedia products and services, provision of technical assistance, creation of technical documentation, and the administration and management of information and communication systems. Mastery of information and communication technologies is the foundation for all successful business organizations today. Persons with expertise in information and communication technologies support and services are in high demand for a variety of positions in business and industry.

Sample occupations associated with this pathway:

- Information Security Analist
- Computer and Information Systems Manager
- Computer User Support Specialist
- Database Administrator
- Document Management Specialist
- Business Intelligence Analyst

B1.0 Identify, and describe the principles of networking and the technologies, models, and protocols used in a network.

B2.0 Identify, describe, and implement network media and physical topologies.

B3.0 Install, configure, and differentiate between common network devices.

B4.0 Demonstrate proper network administration and management skills.

B5.0 Demonstrate how to communicate and interpret information clearly in industry-standard visual and written formats.

B6.0 Use and assess network communication applications and infrastructure.

B7.0 Analyze a customer’s organizational needs and requirements to identify networking needs.

B8.0 Identify security threats to a network and describe general methods to mitigate those threats.

CBE
Competency-Based Education

COMPETENCY-BASED COMPONENTS
for the ***Implementing Cybersecurity Operations*** *Course*

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
A. ORIENTATION AND SAFETY Understand, apply, and evaluate classroom and workplace policies and procedures used in accordance with federal, state, and local safety and environmental regulations. (5 hours)	1. Describe the scope and purpose of the course. 2. Describe the overall course content as a part of the linked Learning Initiative. 3. Describe classroom policies and procedures. 4. Identify classroom and workplace first aid and emergency procedures based on the American Red Cross (ARC) standards. 5. Describe the different occupations in the Information and Communication Technologies industry sector which have an impact on the role of computer technicians. 6. Describe the opportunities available for promoting gender equity and the representation of non-traditional populations in computer technology. 7. Explain the impact of Environmental Protection Agency (EPA) legislation on the Information and Communication Technologies industry sector practices in protecting and preserving the environment. 8. Describe and demonstrate the procedures for contacting proper authorities for the removal of hazardous materials based on the EPA standards. 9. Describe and demonstrate the use of the Material Safety Sheet (MSDS) as it applies to the Information and Communication Technologies industry sector. 10. Describe the California Occupational Safety and Health Administration (Cal/OSHA) and its laws governing information security analysts. 11. Describe how each of the following insures a safe workplace: a) Employees' rights as they apply to job safety b) Employees' obligations as they apply to safety c) Safety laws applying to electrical tools d) Proper use of static straps and static mats 12. Pass the safety exam with 100% accuracy.	**Career Ready Practice:** 1, 2, 4, 7, 8, 12 **CTE Anchor:** Communications: 2.5, 2.6 Technology: 4.1, 4.2, 4.4, 4.5 Problem Solving and Critical Thinking: 5.3, 5.4, 5.5, 5.6, 5.11, 5.12 Ethics and Legal Responsibilities: 8.3, 8.6, 8.8 Technical Knowledge and Skills: 10.1, 10.5, 10.11 **CTE Pathway:** B1.1, B1.3, B1.5, B1.6, B2.1, B3.1, B3.3, B5.1, B8.4
B. ENDPOINT THREAT ANALYSIS AND COMPUTER FORENSICS	1. Interpret the output report of a malware analysis tool such as AMP Threat Grid and Cuckoo Sandbox 2. Describe the Common Vulnerability Scoring System (CVSS) 3. Describe these terms as they are defined in the CVSS 3.0 a) Attack vector b) Attack complexity c) Privileges required d) User interaction e) Scope	**Career Ready Practice:** 1, 2, 8, 12 **CTE Anchor:** Communications: 2.5, 2.6 Technology: 4.1, 4.2, 4.4, 4.5

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
(20 hours)	4. Describe these terms as they are defined in the CVSS 3.0 a) Confidentiality b) Integrity c) Availability 5. Define these items as they pertain to the Microsoft Windows file system 6. Define these items as they pertain to the Microsoft Windows file system a) FAT32 b) NTFS c) Alternative data streams d) MACE e) EFI f) Free space g) Timestamps on a file system 7. Define these terms as they pertain to the Linux file system a) EXT4 b) Journaling c) MBR d) Swap file system e) MAC 8. Compare and contrast three types of evidence a) Best evidence b) Corroborative evidence c) Indirect evidence 9. Compare and contrast two types of disk images a) Altered disk image b) Unaltered disk image 10. Describe the role of attribution in an investigation a) Assets b) Threat actor	Problem Solving and Critical Thinking: 5.3, 5.4, 5.5, 5.6, 5.11, 5.12 Ethics and Legal Responsibilities: 8.3, 8.6, 8.8 Technical Knowledge and Skills: 10.1, 10.5, 10.11 **CTE Pathway:** B1.1, B1.2, B1.3, B1.5, B1.6, B2.1, B3.1, B3.3, B5.1, B8.4
C. NETWORK INSTRUCTION ANAYSIS	1. Interpret basic regular expressions 2. Describe the fields in these protocol headers as they relate to intrusion analysis: a) Ethernet frame b) IPv4 c) IPv6 d) TCP e) UDP f) ICMP g) HTTP 3. Describe NetFlow and explain its use 4. Identify the elements from a NetFlow v5 record from a security event 5. Describe common tools used for packet capture (PCAP) a) Wireshark b) WinPcap c) Npcap	**Career Ready Practice:** 1, 2, 4 **CTE Anchor:** Communications: 2.5 Technology: 4.2, 4.3 Problem Solving and Critical Thinking 5.1, 5.2, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 Technical Knowledge and Skills:

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
(17 hours)	6. Identify these key elements in an intrusion from a given PCAP file a) Source address b) Destination address c) Source port d) Destination port e) Protocols f) Payloads 7. Extract files from a TCP stream when given a PCAP file and Wireshark 8. Interpret common artifact elements from an event to identify an alert a) IP address (source / destination) b) Client and Server Port Identity c) Process (file or registry) d) System (API calls) e) Hashes f) URI / URL 9. Map the provided events to these source technologies a) NetFlow b) IDS / IPS c) Firewall d) Network application control e) Proxy logs f) Antivirus 10. Compare and contrast impact and no impact for these items a) False Positive b) False Negative c) True Positive d) True Negative 11. Interpret a provided intrusion event and host profile to calculate the impact flag generated by Firepower Management Center (FMC)	10.1, 10.8, 10.10 **CTE Pathway:** B1.1, B1.2, B1.6, B4.1 B5.1, B8.4
D. INCIDENT RESPONSE Describe the elements that should be included in an incident response plan as stated in NIST.SP800-61 r2	1. Map elements to these steps of analysis based on the NIST.SP800-61 r2 a) Preparation b) Detection and analysis c) Containment, eradication, and recovery d) Post-incident analysis (lessons learned) 2. Map the organization stakeholders against the NIST IR categories (C2M2, NIST.SP800-61 r2) a) Preparation b) Detection and analysis c) Containment, eradication, and recovery d) Post-incident analysis (lessons learned) 3. Describe the goals of the given CSIRT a) Internal CSIRT b) National CSIRT c) Coordination centers d) Analysis centers	**Career Ready Practice:** 1, 2, 4 **CTE Anchor:** Communications: 2.5 Technology: 4.2, 4.3 Problem Solving and Critical Thinking: 5.1, 5.2, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 Technical Knowledge and Skills:

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
(15 hours)	e) Vendor teams f) Incident response providers (MSSP) 4. Identify these elements used for network profiling a) Total throughput b) Session duration c) Ports used d) Critical asset address space 5. Identify these elements used for server profiling a) Listening ports b) Logged in users/service accounts c) Running processes d) Running tasks e) Applications 6. Map data types to these compliance frameworks a) PCI b) HIPPA (Health Insurance Portability and Accountability Act) c) SOX (Sarbanes-Oxley Act) d) Identify data elements that must be protected with regards to a specific standard (PCI-DSS)	10.6, 10.7 **CTE Pathway:** B1.1, B1.2, B1.5, B1.6, B4.1, B4.3, B5.1, B8.2, B8.4
E. DATA AND EVENT ANALYSIS (15 hours)	1. Describe the process of data normalization 2. Interpret common data values into a universal format 3. Describe 5-tuple correlation 4. Describe the 5-tuple approach to isolate a compromised host in a grouped set of logs 5. Describe the retrospective analysis method to find a malicious file, provided file analysis report 6. Identify potentially compromised hosts within the network based on a threat analysis report containing malicious IP address or domains 7. Map DNS logs and HTTP logs together to find a threat actor 8. Map DNS, HTTP, and threat intelligence data together 9. Identify a correlation rule to distinguish the most significant alert from a given set of events from multiple data sources using the firepower management console 10. Compare and contrast deterministic and probabilistic analysis	**Career Ready Practice:** 1, 2, 4 **CTE Anchor:** Communications: 2.5 Technology: 4.2, 4.3 Problem Solving and Critical Thinking: 5.1, 5.2, 5.3, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 Technical Knowledge and Skills: 10.1, 10.8, 10.10 **CTE Pathway:** B1.1, B1.6, B4.1, B5.1, B8.4
F. INCIDENT HANDLING	1. Classify intrusion events into these categories as defined by the Cyber Kill Chain Model a) Reconnaissance b) Weaponization c) Delivery d) Exploitation	**Career Ready Practice:** 1, 2, 4 **CTE Anchor:** Communications: 2.5

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
(10 hours)	e) Installation f) Command and control g) Action on objectives 2. Apply the NIST.SP800-61 r2 incident handling process to an event 3. Define these activities as they relate to incident handling a) Identification b) Scoping c) Containment d) Remediation e) Lesson-based hardening f) Reporting 4. Describe these concepts as they are documented in NIST SP800-86 a) Evidence collection order b) Data integrity c) Data preservation d) Volatile data collection a) Apply the VERIS schema categories to a given incident	Technology: 4.2, 4.3 Problem Solving and Critical Thinking: 5.1, 5.2, 5.3, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 Technical Knowledge and Skills: 10.1, 10.8, 10.10 **CTE Pathway:** B1.1, B1.6, B4.1, B5.1, B8.4
G. EMPLOYABILITY SKILLS Understand, apply, and evaluate the employability skills required in the Cypbersecurity field. Understand the requirements and procedures for obtaining a CCNA CyberOps certification (8 hours)	1. Summarize employers' requirements. 2. Identify potential employers through traditional and internet sources. 3. Describe the role of social media in job search. 4. Design sample résumés and covers letters. 5. Explain the importance of filling out a job application legibly, with accurate and complete information. 6. Describe the common mistakes that are made on job applications. 7. Complete sample job application forms correctly. 8. State the importance of enthusiasm in the interview and on a job. 9. State the importance of appropriate appearance in the interview and on a job. 10. State the importance of the continuous upgrading of job skills. 11. Describe customer service as a method of building permanent relationships between the organization and the customer. 12. Describe and Demonstrate appropriate interviewing techniques. 13. Identify the informational materials and resources needed to be successful in an interview. 14. Design sample follow-up letters. 15. Describe and demonstrate appropriate follow-up procedures.	**Career Ready Practice:** 1, 2, 3, 4, 6, 7, 8, 9, 11, 12 **CTE Anchor:** Communications: 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8 Career Planning and Management: 3.1, 3.2, 3.3, 3.4, 3.8 Technology: 4.5 **CTE Pathway:** B7.1, B7.3

SUGGESTED INSTRUCTIONAL MATERIALS and OTHER RESOURCES

TEXTS AND SUPPLEMENTAL BOOKS

Omar Santos, Joseph Muniz CCNA Cyber Ops SECOPS 210-255 Official Cert Guide. Cisco Press, 2017, ISBN-10: 1-58714-703-3

RESOURCES

Employer Advisory Board Meetings

CTE Foundation Standards
http://www.cde.ca.gov/ci/ct/sf/documents/ctestandards.pdf
http://www.cde.ca.gov/be/st/ss/documents/ctestandards.doc

TEACHING STRATEGIES and EVALUATION

METHODS AND PROCEDURES

A. Lecture and discussion

B. Multimedia presentations

C. Demonstrations and Hands-on Labs

D. Individualized instruction

E. Peer teaching

F. Role-playing

G. Guest speakers

H. Field trips and field study experiences

I. Projects

EVALUATION

SECTION A – Orientation and Safety – Pass the safety test with 100% accuracy.

SECTION B – Endpoint Threat Analysis and Computer Forensics - Pass all assignments and exams on Endpoint Threat Analysis and Computer Forensics with a minimum score of 80% or higher.

SECTION C – Network Intrusion Analysis – Pass all assignments and exams on Network Intrusion Analysis with a minimum score of 80% or higher.

SECTION D – Incident Response – Pass all assignments and exams on Incident Response with a minimum score of 80% or higher.

SECTION E – Data and Event Analysis – Pass all assignments and exams on Data and Event Analysis with a minimum score of 80% or higher.

SECTION F – Incident Handling – Pass all assignments and exams on Incident Handling analysis with a minimum score of 80% or higher.

SECTION G – Employability Skills – Pass all assignments and exams on employability skills with a minimum score of 80% or higher.

Statement for Civil Rights

All educational and vocational opportunities are offered without regard to race, color, national origin, gender, or physical disability.