Course ID: CIMS 165
Cat ID: 103007.00
State ID: CCC000608974

College:	A	Saddleback College
Division/School:	BS	Business Science
Department:	CIM	Computer Information Management
Program:	CIMNAD	Network Administrator
Subject:	CIMNAD	Network Administrator

O F F I C I A L C O U R S E O U T L I N E

HISTORY AND STATUS

Course Status: A Active (Fully Approved)
Course Originator: Tom DeDonno

Board of Trustees	10/28/19
State Approval	11/07/19
Curriculum Committee Approval	09/12/19
Division Approval	09/12/19
Tech Review Approval	09/12/19

Technical Change Date:

Technical Change Comment:

Comments:

BRIEF DESCRIPTION

Short Title: CISCO CCNA CYBER OP
Full Title: CYBERSECURITY OPERATIONS- CISCO CCNA CYBER OPS

BRIEF DESCRIPTION

Catalog Description:

This course equips students with the knowledge and skills needed by today's organizations that are challenged with rapidly detecting cybersecurity breaches and effectively responding to security incidents. The student would be part of a team of people in Security Operations Centers (SOC’s) keeping a vigilant eye on security systems, protecting their organizations by detecting and responding to cybersecurity threats. CCNA Cyber Ops prepares candidates to begin a career working with associate-level cybersecurity analysts within security operations centers.. Includes preparation for Cisco's CCNA CyberOps exam.

Prerequisite:

None

Enrollment Limitation:

None

Corequisite:

None

Recommended Preparation:

CIMS 130 and CIMN 120

COURSE FUNCTIONS

Course Prior to:	Y	Not Applicable
Course Classification:	Y	Credit Course
SC/IVC GE Code:	NA - Not Applicable	
CSU GE Code:	NA	Not Applicable
IGETC GE Code:	NA - Not Applicable	
UC Transferable Course:	N	No UC credit
Comparable SC/IVC:		
Comparable CSU:	CSU CSU Monterey Bay CST 282 - Introduction to Network Security	
Comparable UC:		
Comparable CCC Baccalaureate:		
TOP Code:	0708.10	Network Administrator
SAM Code:	C	Clearly Occupational
CAN Number:		
CID Number:		

COURSE OPTIONS

Grading Option:	GR	Letter Grade or Pass/No Pass
Open Entry:	N	No
Fixed, Optional or Variable Units:	F	Fixed Units
Repeatability Status:	N	No
Repeatability Model:		
Repeatability Limit:	0	
Cross-Listed Courses:	NONE	
Cross-Listed Parent:	No	

COURSE VALUES

Method of Instruction:	L-L	Lecture/Lab Combination	
Maximum Enrollment:	40	Maximum WSCH:	200
Average Enrollment:	22	Average WSCH:	110

	Lecture	Lab	Learn Ctr	Total
WFCH	2.00	3.00	0.00	5.00
TFCH	33.20	49.80	0.00	83.00
TSCH	33.20	49.80	0.00	83.00
LHE	2.00	2.50	0.00	4.50
FTEF	13.33	16.67	0.00	30.00
UNITS	2.00	1.00	0.00	3.00

Schedule Description:

This course equips students to work in Security Operations Centers (SOC's) with the knowledge and skills needed by today's organizations that are challenged with rapidly detecting cybersecurity breaches and effectively responding to security incidents. Includes preparation for the Cisco's CCNA CyberOps exam.

COURSE CONTENT
(Topics Covered)

Lecture Topics:

I. Cybersecurity and the Security Operations Center
   A. The Danger - Explain why networks and data are attacked.
   B. Fighters in the War Against Cybercrime - Explain how to prepare for a career in Cybersecurity operations.

II. Windows Operating System
   A. Windows Overview - Explain the operation of the Windows Operating System.
   B. Windows Administration - Explain how to secure Windows endpoints.

III. Linux Operating System
   A. Using Linux - Perform basic operations in the Linux shell.
   B. Linux Administration - Perform basic Linux administration tasks.
   C. Linux Clients - Perform basic security-related tasks on a Linux host.

IV. Network Protocols and Services
   A. Network Protocols - Explain how protocols enable network operations.
   B. Ethernet and Internet Protocol(IP) - Explain how the Ethernet and IP protocols support network communication.
   C. Connectivity Verification - Use common testing utilities to verify and test network connectivity.
   D. Address Resolution Protocol- Explain how the address resolution protocol enables communication on a network.
   E. The Transport Layer and Network Services - Explain how transport layer protocols and network services support network functionality.
   F. Network Services - Explain how network services enable network functionality.

V. Network Infrastructure
   A. Network Communication Devices - Explain how network devices enable wired and wireless network communication.
   B. Network Security Infrastructure - Explain how devices and services are used to enhance network security.
   C. Network Representations - Explain how networks and network topologies are represented.

VI. Principles of Network Security
   A. Attackers and Their Tools - Explain how networks are attacked.
   B. Common Threats and Attacks - Explain the various types of threats and attacks.

VII. Network Attacks: A Deeper Look
   A. Observing Network Operation - Explain network traffic monitoring.
   B. Attacking the Foundation - Explain how TCP/IP vulnerabilities enable network attacks.
   C. Attacking What We Do - Explain how common network applications and services are vulnerable to attack.

VIII. Protecting the Network
   A. Understanding Defense - Explain approaches to network security defense.
   B. Access Contr ol- Explain access contr olas a method of protecting a network.
   C. Network Firewalls and Intrusion Prevention - Explain how firewalls and other devices prevent network intrusions.
   D. Content Filtering - Explain how content filtering prevents unwanted data from entering the network.
   E. Threat Intelligence - Use various intelligence sources to locate current

security threats.

IX. Cryptography and the Public Key Infrastructure
  A. Cryptography - Use tools to encrypt and decrypt data.
  B. Public Key Cryptography - Explain how the public key infrastructure (PKI) supports network security.

X. Endpoint Security and Analysis
  A. Endpoint Protection - Use a tool to generate a malware analysis report.
  B. Endpoint Vulnerability Assessment - Classify endpoint vulnerability assessment information.

XI. Security Monitoring
  A. Technologies and Protocols - Explain how security technologies affect security monitoring.
  B. Log Files - Explain the types of log files used in security monitoring

XII. Intrusion Data Analysis
  A. Data Collection - Explain how security-related data is collected.
  B. Data Preparation - Arrange a variety of log files in preparation for intrusion data analysis.
  C. Data Analysis - Analyze intrusion data to determine the source of an attack.

XIII. Incident Response and Handling
  A. Incident Response Models - Apply incident response models to an intrusion event.
  B. CSIRTs and NIST 800-61r2 - Apply standards specified in NIST 800-61r2 to a computer security incident.
  C. Case-Based Practice - Given a set of logs, isolate a threat actor and recommend an incident response plan.

Lab/Learning Center Content:

I. Installing virtual machines.
II. Utilizing Windows Operating System to illustrate various tools for analyzing cybersecurity attacks.
III. Analyzing network security alerts.
IV. Implementing methods to prevent malicious attacks.
V. Analyzing network protocols and services.

COURSE CONTENT
(Learning Objectives)

Students participating in this class will:

1. Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events.
2. Explain the role of the Cybersecurity Operations Analyst in the enterprise.
3. Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses.
4. Explain the features and characteristics of the Linux Operating System.
5. Analyze the operation of network protocols and services.
6. Explain the operation of the network infrastructure.
7. Classify the various types of network attacks.
8. Use network monitoring tools to identify attacks against network protocols and services.
9. Use various methods to prevent malicious access to computer networks, hosts, and data.
10. Explain the impacts of cryptography on network security monitoring.
11. Explain how to investigate endpoint vulnerabilities and attacks.
12. Evaluate network security alerts.
13. Analyze network intrusion data to identify compromised hosts and vulnerabilities.
14. Apply incident response models to manage network security incidents

COURSE CONTENT
(Student Learning Outcomes)

Students completing this course satisfactorily will be able to:

1. Identify various roles in a security operations center (SOC).
2. Explain various security alerts.
3. Identify various methods to prevent malicious access.

COURSE CONTENT
(Methods of Evaluation)

Evaluation of the student will be based upon the following items:

1. Writing Assignments
   short answers
   other (specify)
   a. Students will be evaluated on their performance on written examinations which require students to demonstrate knowledge of cyber operations in a security operation center.

2. Problem Solving Demonstrations
   quizzes
   other (specify)
   a. Students will be evaluated on computer assignments requiring students to demonstrate proficiency in the use of various security programs in analyzing security threats.

3. Skill Demonstrations
   class performance(s)
   other (specify)
      a. Students will be evaluated on computer assignments requiring students to demonstrate proficiency in the use of various security programs in analyzing security threats, network protocol attacks, and intrusion data.

4. Examinations
   multiple choice, true/false
   other (specify)
      a. Students will be evaluated on their performance on written examinations which require students to demonstrate knowledge of cybersecurity analysts in the enterprise.

5. Other
   other (specify)
      a. Students will be evaluated on presentations relating to cyber operations.

COURSE CONTENT
(In and Out-of-Class Assignments)

1. Typical Reading Assignments:
   Students will be expected to understand and critique college level technical documents or the equivalent. Reading assignments may include but are not limited to the following:

   a. Assigned Computer-Based courseware
   b. Technical papers
   c. Technical Web sites
   d. Current PDF based textbooks.

2. Typical Writing Assignments:
   Writing assignments will pertain directly to the course topics and may include but are not limited to the following:

   a. Examinations and quizzes
   b. Lab exercises and problem simulations

3. Typical Oral Assignments:
   Class discussions

COURSE CONTENT
(Other Requirements)

Textbooks / Supplies:
Omar Santos, Joseph Muniz, CCNA Cyber Ops SECOPS 210-255 Pearson uCertify Course and Labs and Textbook Bundle, 1st Ed. Cisco Press. 2017
Cisco Academy, CCNA Cybersecurity Operations NetAcad Companion Guide, 1st Ed. Cisco Press. 2018
Cisco Academy, CCNA Cybersecurity Operations NetAcad Companion Guide Lab Manual, 1st Ed. Cisco Press. 2018

Material Fees: $ 0.00 Transaction Code:

VALIDATION
(Corequisite, Limitation on Enrollment,
Prerequisite and Recommended Preparation)

Recommended Preparation:

CIMN 120

I. Describe computer networks and differentiate the devices and services used to support communications in data networks and the Internet.
II. Describe the role of protocol layers in data networks and how they are used.
III. Evaluate the importance of addressing and naming schemes at various layers of data networks in IPv4 and IPv6 environments.
IV. Design, calculate and apply subnet masks and addresses to fulfill given requirements in IPv4 and IPv6 networks.
V. Explain fundamental Ethernet concepts such as media, services, and operations.
VI. Build a simple Ethernet network using hardware components of computer networks such as routers and switches.
VII. Compose the Cisco command-line interface (CLI) commands to perform basic router and switch configurations.
VIII. Experiment and Describe how network software utilities are used to communicate over a network, verify network operations and analyze data traffic.
IX. Identify various network strategies and topologies.
X. Describe how data is transmitted over a network.
XI. Identify the OSI model and describe how communication layers interact.
XII. Identify the basic functions of network management.
XIII. Identify future possibilities for computers and computer networks.
XIV. Experiment with common network utilities to verify small network operations and analyze data traffic.

CIMS 130

I. Introduction to Information Systems Security.
II. Explain social engineering, malware, and social engineering attacks.
III. Application and network attacks.
IV. List security ramifications, vulnerability assessment, mitigating attacks and costs of intrusion.
V. Host, application, and data security.
VI. Network and specifically email security.
VII. Administering a secure network.
VIII. Wireless network security.
IX. Access control fundamentals.
X. Authentication and account management.
XI. Apply concepts of using cryptography both basic and advanced.
XII. Describe business continuity, risk mitigation, and the disaster recovery planning process.
XIII. Analyze how intrusion detection systems operate.
XIV. Explain network hardening.
XV. Describe the purpose of honeypots.