Course ID: CIMS 155
Cat ID: 668185.00
State ID: CCC000608973

College:	A	Saddleback College
Division/School:	BS	Business Science
Department:	CIM	Computer Information Management
Program:	CIMECO	E-Commerce
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	09/19/19
Division Approval	09/19/19
Tech Review Approval	09/19/19

Technical Change Date:

Technical Change Comment:

Comments:

BRIEF DESCRIPTION

Short Title: COMPTIA CYSA+
Full Title: CYBERSECURITY ANALYSIS - COMPTIA CYSA+

BRIEF DESCRIPTION

Catalog Description:

This course provides preparation for the DOD recommended intermediate level CompTIA CySa+ certification exam. In this course students will learn how to configure and use threat detection tools, perform data analysis, and interpret the results to identify vulnerabilities, threats, and risks to an organization with the end goal of securing and protecting applications and systems within an organization. The course covers skills used by IT security analysts, vulnerability analysts, or threat intelligence analysts with a technical, "hands-on" focus on IT security analytics.

Prerequisite:

None

Enrollment Limitation:

None

Corequisite:

None

Recommended Preparation:

CIMN 120 and CIMS 130

COURSE FUNCTIONS

Course Prior to:	Y	Not Applicable
Course Classification:	Y	Credit Course
SC/IVC GE Code:	NA - Not Applicable	
CSU GE Code:	TR	Transferable as an elective-does not fit GE pattern
IGETC GE Code:	NA - Not Applicable	
UC Transferable Course:	N	No UC credit
Comparable SC/IVC:		
Comparable CSU:	CSU CSU San Bernardino IST 275 - Information Networking and 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:	45	Maximum WSCH:	225
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 prepares students for CompTIA CySa+ exam. This course covers configuration and use threat detection tools, identification and analysis of vulnerabilities, threats, and risks to an organization with the end goal of securing and protecting an organization's applications and systems.

COURSE CONTENT
(Topics Covered)

Lecture Topics:

I. Applying Reconnaissance Techniques
  A. Open Source Intelligence
  B. Active Reconnaissance
  C. Special Considerations
  D. Tools of the Trade
II. Analyzing the Results of Reconnaissance
  A. Data Sources
  B. Point-in-Time Analysis
  C. Correlation Analysis
  D. Tools of the Trade
III. Responding to Network-Based Threats
  A. Network Segmentation
  B. Honeypots and Honeynets
  C. ACLs
  D. Endpoint Security
  E. Group Policies
  F. Device Hardening
  G. Network Access Control
IV. Securing a Cooperate Network
  A. Penetration Testing
  B. Reverse Engineering
  C. Training and Exercises
  D. Risk Evaluation
V. Implementing Vulnerability Management Processes
  A. Vulnerability Management Requirements
  B. Common Vulnerabilities
  C. Frequency of Vulnerability Scans
  D. Tool Configuration
VI. Vulnerability Scanning
  A. Execute Scanning
  B. Generate Reports
  C. Remediation
  D. Ongoing Scanning and Continuous Monitoring
  E. Analyze Reports from a Vulnerability Scan
  F. Validate Results and Correlate Other Data Points
VII. The Incident Response Process
  A. A Cast of Characters
  B. Response Techniques
  C. Communication Processes
VIII. Determining the Impact of Incidents
  A. Threat Classification
  B. Factors Contributing to Incident Severity and Prioritization
IX. Preparing the Incident Response Toolkit
  A. Digital Forensics
  B. Forensic Investigation Suite
  C. Building Your Forensic Kit
X. Selecting the Best Course of Action
  A. Introduction to Diagnosis
  B. Network-Related Symptoms

C. Host-Related Symptoms
D. Application-Related Symptoms

XI. Frameworks, Policies, Controls, and Procedures
A. Security Frameworks
B. Policies and Procedures
C. Controls
D. Regulatory Compliance
E. Verification and Quality Control

XII. Identity and Access Management
A. Security Issues Associated with Context-Based Authentication
B. Security Issues Associated with Identities
C. Security Issues Associated with Identity Repositories
D. Security Issues Associated with Federation and Single Sign-On
E. Exploits

XIII. Putting in Compensating Controls
A. Security Data Analytics
B. Manual Review
C. Defense in Depth

XIV. Secure Software Development
A. The Software Development Lifecycle
B. Secure Software Development
C. Best Practices
D. Center for Internet Security

XV. Tool Sets
A. Preventive Tools
B. Collective Tools
C. Analytical Tools
D. Exploitative Tools
E. Forensic Tools

Lab/Learning Center Content:

I. Configuring and using threat detection tools
II. Analyzing cyber attack data
III. Using the incident response process
IV. Using the forsenics incident response
V. Identifying risks to an organization

COURSE CONTENT
(Learning Objectives)

Students participating in this class will:

1. Apply environmental reconnaissance techniques using appropriate tools and processes.
2. Analyze the results of a network reconnaissance.
3. Implement or recommend the appropriate response and countermeasure for a network-based threat.
4. Explain the purpose of practices used to secure a corporate environment.
5. Implement an information security vulnerability management process.
6. Analyze the output resulting from a vulnerability scan.
7. Compare and contrast common vulnerabilities found in the following targets within an organization.
8. Distinguish threat data or behavior to determine the impact of an incident.
9. Prepare a toolkit and use appropriate forensics tools during an investigation.
10. Explain the importance of communication during the incident response process.
11. Analyze common symptoms to select the best course of action to support incident response.
12. Summarize the incident recovery and post-incident response process.
13. Explain the relationship between frameworks, common policies, controls, and procedures.
14. Use data to recommend remediation of security issues related to identity and access management.
15. Review security architecture and make recommendations to implement compensating controls.
16. Use application security best practices while participating in the Software Development Life Cycle (SDLC).
17. Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies.

COURSE CONTENT
(Student Learning Outcomes)

Students completing this course satisfactorily will be able to:

1. Identify and configure threat detection tools.
2. Explain threats to an organization.
3. Interpret threat detection results.

COURSE CONTENT
(Methods of Evaluation)

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

1. Writing Assignments
   short answers
   other (specify)
   a. Evaluation of weekly quizzes with short answers covering the previous lecture topic including incident reporting, data

detection tools, vulnerability scanning, policies and procedures.

2. Problem Solving Demonstrations
   other (specify)
   a. Evaluation of problem solving exercises using cybersecurity analysis in protecting, detecting vulnerabilities and resolving cyber attacks.

3. Skill Demonstrations
   other (specify)
   a. Final project assignments that require student to configure data threat detection tools and analyze the cyber attacks that these tools detect.

4. Examinations
   other (specify)
   a. Practice examination or test questions preparation for CompTIA CySa+ exam.

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

1. Typical Reading Assignments:
   Reading assignments in college-level textbook covering cybersecurity analysis

2. Typical Writing Assignments:
   Cybersecurity incident and forensic reports

3. Typical Oral Assignments:
   Class discussions on course topics

4. Typical Other Assignments:
   Students will explore various means to protect and detect cyber attacks in a corporate system and application environment.

COURSE CONTENT
(Other Requirements)

Textbooks / Supplies:
Chapple, M., & Seidl, D., CompTIA CySA+ Practice Tests: Exam CS0-001, 1st Ed. Sybex. 2018
Maymi, F., Chapman, B.,, CompTIA CySA+ Cybersecurity Analyst Certification All-In-One Exam Guide (CS0-001), 1st Ed. McGraw-Hill Education. 2017

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.