SAN DIEGO COMMUNITY COLLEGE DISTRICT
CONTINUING EDUCATION
COURSE OUTLINE

SECTION I

SUBJECT AREA AND COURSE NUMBER

COMP 656

COURSE TITLE

CYBER INCIDENT RESPONSE INTRO

TYPE COURSE

NON-FEE VOCATIONAL

CATALOG COURSE DESCRIPTION

This course covers cybersecurity incident response planning, tools and techniques. Students will build a formal incident response handling program. Students use tools to contain, cleanup, recover and prepare a post incident report. Topics include forensic tools, their appropriate use, and analysis of the symptoms of an incident. The purpose and importance of communication and role-based responsibilities will be integrated throughout the course. (FT)

LECTURE/LABORATORY HOURS

45

ADVISORIES

COMP 655 Cyber Threat and Vulnerability or equivalent

RECOMMENDED SKILL LEVEL

Possess a 12th grade reading level; ability to communicate effectively in the English language; knowledge of math concepts at the 8th grade level and computer literacy.

INSTITUTIONAL STUDENT LEARNING OUTCOMES

1. Social Responsibility
   SDCE students demonstrate interpersonal skills by learning and working cooperatively in a diverse environment.
2. Effective Communication
   SDCE students demonstrate effective communication skills.
3. Critical Thinking
   SDCE students critically process information, make decisions, and solve problems independently or cooperatively.

INSTITUTIONAL STUDENT LEARNING OUTCOMES (CONTINUED)

4. Personal and Professional Development
   SDCE students pursue short-term and life-long learning goals, mastering necessary skills and using resource management and self advocacy skills to cope with changing situations in their lives.

COURSE GOALS

1. Learn about the roles and responsibilities of a computer security incident response team.
2. Gain an understanding of threat behavior and its impact.
3. Learn about threat data, including classification and impact.
4. Learn about the common tools found in a forensic investigation suite.
5. Explore the purpose and importance of communication during incident response.
6. Learn to recognize the symptoms of a security incident.
7. Gain an understanding of the post-incident response process and summary report.

COURSE OBJECTIVES

Upon successful completion of this course students will be able to:

1. Describe the roles and responsibilities of a computer security incident response team.
2. Distinguish threat data or behavior and determine the impact of an incident.
3. Identify and explain the purpose of common digital forensics tools used in investigations.
4. Prepare a toolkit and use appropriate forensics tools during an investigation.
5. Explain the importance of communication during the incident response process.
6. Analyze common symptoms of a security incident.
7. Based on symptom analysis, determine the appropriate course of action to support incident response.
8. Summarize the incident recovery and post-incident response process.

SECTION II

COURSE CONTENT AND SCOPE

1. Incident Impact, Threat Data, and Behavior
   - 1.1. Threat Classification
     - 1.1.1. Known and unknown threats
     - 1.1.2. Zero day threats
     - 1.1.3. APT (advanced persistent threat)
   - 1.2. Scope of impact
     - 1.2.1. Downtime
     - 1.2.2. Recovery time
     - 1.2.3. Data integrity
     - 1.2.4. Economic
     - 1.2.5. System process criticality
   - 1.3. Data Types
     - 1.3.1. PII (personally identifiable information)
     - 1.3.2. PHI (personal health information)

COURSE CONTENT AND SCOPE (CONTINUED)

1.3.3. Payment card information
1.3.4. Intellectual property
1.3.5. Corporate confidential: accounting, mergers and acquisitions

2. Forensic Toolkit Preparation and Use
   2.1. Forensics toolkit
      2.1.1. Digital forensics workstation
      2.1.2. Write blockers
      2.1.3. Cables
      2.1.4. Drive adapters
      2.1.5. Wiped removable media
      2.1.6. Cameras
      2.1.7. Crime tape
      2.1.8. Tamper-proof seals
      2.1.9. Documentation such as chain of custody, incidence response plan, incident form, call list, escalation list
   2.2. Forensics investigation suite
      2.2.1. Imaging utilities
      2.2.2. Analysis utilities
      2.2.3. Chain of custody
      2.2.4. Hashing utilities
      2.2.5. OS (operating system) and process analysis
      2.2.6. Mobile device forensics
      2.2.7. Password crackers
      2.2.8. Cryptography tools
      2.2.9. Log viewers
3. Importance of Communication
   3.1. Stakeholders
      3.1.1. HR
      3.1.2. Legal
      3.1.3. Marketing
      3.1.4. Management
   3.2. Communication processes
      3.2.1. Limit communication to trusted parties
      3.2.2. Disclosure based on regulatory and legislative requirements
      3.2.3. Prevent inadvertent release of information
      3.2.4. Secure method of communication
   3.3. Role-based responsibilities
      3.3.1. Technical
      3.3.2. Management
      3.3.3. Law enforcement
      3.3.4. Retain incident response provider
4. Symptom Analysis and Actions
   4.1. Common network-related symptoms
      4.1.1. Bandwidth consumption
      4.1.2. Beaconing
      4.1.3. Irregular peer-to-peer communication

COURSE CONTENT AND SCOPE (CONTINUED)

- 4.1.4. Rogue devices on the network
- 4.1.5. Scan sweeps
- 4.1.6. Unusual traffic spikes
- 4.2. Common host-related symptoms
  - 4.2.1. Processor consumption
  - 4.2.2. Memory consumption
  - 4.2.3. Drive capacity consumption
  - 4.2.4. Unauthorized software
  - 4.2.5. Malicious processes
  - 4.2.6. Unauthorized changes
  - 4.2.7. Unauthorized privileges
  - 4.2.8. Data exfiltration
- 4.3. Common application-related symptoms
  - 4.3.1. Anomalous activity
  - 4.3.2. Introduction of new accounts
  - 4.3.3. Unexpected output
  - 4.3.4. Unexpected outbound communication
  - 4.3.5. Service interruption
  - 4.3.6. Memory overflows

5. Incident Recovery and Post-Incident Response Summarization
   - 5.1. Containment
     - 5.1.1. Segmentation
     - 5.1.2. Isolation
     - 5.1.3. Removal
     - 5.1.4. Reverse engineering
   - 5.2. Eradication
     - 5.2.1. Sanitization
     - 5.2.2. Reconstruction and reimaging
     - 5.2.3. Secure disposal
   - 5.3. Validation
     - 5.3.1. Patching
     - 5.3.2. Permissions
     - 5.3.3. Scanning
     - 5.3.4. Security monitoring logging verification
   - 5.4. Corrective actions
     - 5.4.1. Lessons learned report
     - 5.4.2. Change control process
     - 5.4.3. Update incident response plan
   - 5.5. Incident summary report

APPROPRIATE READINGS

Readings may include, but are not limited to, textbooks, manuals, periodicals, instructor-written materials, and websites related to cyber incident response.

WRITING ASSIGNMENTS

Appropriate writing assignments may include, but are not limited to, preparing text for an assigned project, documenting all laboratories and project work, and completing all written assigned reports, such as developing an incident communications plan.

OUTSIDE ASSIGNMENTS

Outside assignments may include, but are not limited to, reading texts and reference resources; research as needed to complete projects, such as determining and prioritizing factors that contribute to incident severity; and organizing and preparing written answers to assigned questions.

APPROPRIATE ASSIGNMENTS THAT DEMONSTRATE CRITICAL THINKING

Assignments which exhibit critical thinking may include analysis and evaluation of assigned text and reference resources, and utilize this analysis in classroom discussions, as well as completing lab activities. Appropriate assignments may include performing network scans and preparing a service issue response plan. Students must select appropriate forensic tools and employ appropriate methods needed to complete laboratory assignments, including recovering volumes or drives.

EVALUATION

A student’s grade will be based on multiple measures of performance and will include evaluation of student’s ability to:

1. Perform in a variety of activities and assignments related to the course objectives.
2. Complete written and practical examinations.
3. Contribute to class and group discussions.
4. Maintain attendance and punctuality per current policy.
5. Demonstrate ability to work independently and as a team member.
6. Demonstrate troubleshooting skills.

Upon successful completion of each course in the program, a Certificate of Course Completion will be issued. Upon successful completion of all courses included in the program, a Certificate of Program Completion will be issued.

METHOD OF INSTRUCTION

Methods of instruction may include, but are not limited to, lectures, self-paced lab, demonstrations, individualized study, use of audio-visual aids, group/team work, tutorials, outside assignments, guest lectures, field trips, and guided student job assignments. This course, or sections of this course, may be offered through distance education.

TEXTS AND SUPPLIES

CompTIA Cybersecurity Analyst (CSA+) Study Guide: Exam CS0-001, Michael J. Chapple, David Seidl, Sybex, current edition
CompTIA Cybersecurity Analyst (CSA+) Cert Guide (Certification Guide), Troy McMillan, Pearson, current edition
CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001), Fernando Maymi, Brent Chapman, McGraw Hill, current edition

Web Resources:
ITPRO.TV, https://itpro.tv/course-library/cybersecurity-analyst-csa/overview70770;
CompTIA Marketplace, https://www.comptiastore.com/CompTIA-Cybersecurity-Analyst-CSA-eBook-Labs-p/pl720ebk.htm;
CYBRARY, https://www.cybrary.it/catalog/practice_labs/comptia-cybersecurity-analyst-csa

Supplies: Journal (composition book), USB Drive or other storage media

PREPARED BY: Richard Gholson DATE: February 7, 2018

REVISED BY: ______________________ DATE: ______________

Instructors must meet all requirements stated in Policy 3100 (Student Rights, Responsibilities and Administrative Due Process), and the Attendance Policy set forth in the Continuing Education Catalog.

REFERENCES:

San Diego Community College District Policy 3100
California Community Colleges, Title 5, Section 55002
Continuing Education Catalog