TSC - CCSO®

TRAINING COURSE

CCSO® - Certified Cyber Security Operator

Titans Security College

Index

Course Overview

This course is for computer incident response team (CSIRT) or Security Operation Center (SOC) operators, or any other technical staff who have little or no incident handling experience. It provides a basic introduction to the main incident handling tasks and critical thinking skills that will help an incident handler perform their daily work. It is highly recommended to those new to incident handling work.
The course is designed to provide insight into the world that an incident handler may perform. It will provide an overview of the incident handling arena, including CSIRT services, intruder threats, and the nature of incident response activities.

Course Description

Course Objectives

Upon successfully completion of the CCSO® course, each participant will be armed with the knowledge, tools, and processes required in conducting incident response, producing professional reports that withstand legal scrutiny, and participating in an incident handling and investigation process. Specifically, students will posses' relevant knowledge and real-world hands-on skills on the following topics:

- Understanding the CSIRT environment and basic handling management processes
- CSIRT code of conduct
- Understanding security tools and technologies used by CSIRT's
- Identifying and gathering critical information
- Recognizing signs of attacks
- Detecting and analyzing cyber security incidents
- Incident handling and response
- Cyber intelligence
- Security technologies involved in a SOC operation
- Incident Response metrics
- Cyber security threats and risks
- Coordinating response and disseminating information
- Working with law enforcements

Course Format

The CCSO® course is built in a unique way based on years of knowledge and proven experience.
The course is based on an Instructor - led format (lectures, exercises, case-studies and labs).
The course includes:

- Interactive presentations by cyber security, forensics and incident response experts.
- Hands-on on different topics, performing forensics and incident response processes.
- Examining different case-studies, based on real cases and investigations.
- Exercise (both in class- led by the instructor, and outside the class - independent or in small groups).

Course Structure and Format

Course Duration

The course duration is 200 academic hours, divided as the following:

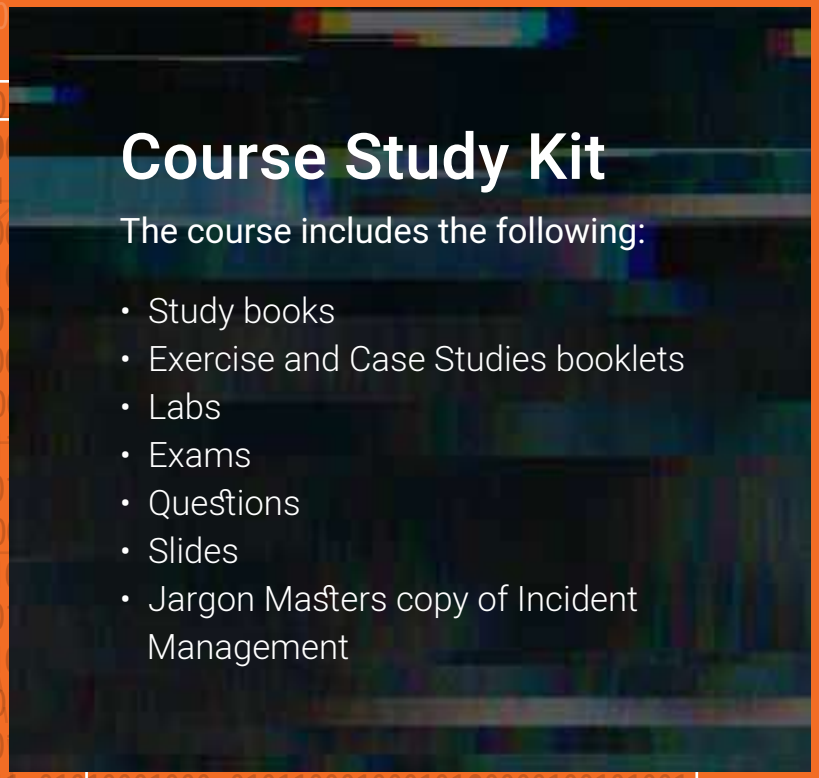
- 150 hours - theoretical and practical curriculum
- 50 hours - practice with built-in labs and table-top exercise.

Target Audience

SOC operators, new CERT/CSIRT team members, experienced CSIRT staff who would like to benchmark their CSIRT processes and skill sets against best practices security experts, IT experts, incident handlers, threat hunters and anyone who would like to learn about basic incident handling functions and activities.

Course Prerequisites

- A minimum of one year in the IT domain (system, network, security).
- Sound knowledge of OS's, security technologies, TC/IP.



Course Syllabus

Module 1 - Intro

- Cyber Security
- Cyber Warfare
- Cyber Threats and Vulnerabilities

Module 2 - Overview of Computer Crime

- How computer crime affects digital forensics
- Types of computer crimes
- Attacker Types
- Attack Methods
- Case Studies

Module 3 - SOC Operation

- SOC models and operation
- SOC Services
- SOC guidelines

Module 4 - SOC Technologies

- Endpoint Security tools
- Network Security Tools
- Gateway Security Tools
- SIEM technologies
- Cyber Security Technologies

Module 5 - SOC Roles and Responsibilities

- The main Roles in Incident Management
  - Threat Hunters
  - Security Analysts
  - Incident Handlers
  - Incident Management
  - Security operators
  - CERT/CSIRT team
- The role of the Auditor in incident handling

Module 6 - Cyber Intelligence

- Understanding Cyber and Threat Intelligence
- The need for Cyber Intelligence
- Types of Intelligence
  - HUMINT (Human Intelligence)
  - OSINT (Open Source Intelligence)
  - SIGINT (Signals Intelligence)
  - COMINT (Communications Intelligence)
  - ELINT (Electronic Intelligence)
  - TECHINT (Technical Intelligence)
  - Other Sources of Intelligence (MEDINT, MASINT, IMINT, FISINT, etc.)
- Cyber Intelligence lifecycle
- Integrating Cyber Intelligence, Security and Operations
- Developing a strategic cyber intelligence capability
- Cyber Intelligence roles and responsibilities
- Case Studies
- Exercise

Module 7 - Digital Forensics

- What is Computer Forensics?
- Understanding the field of Digital Forensics
- What is Digital Evidence
- Challenges for Digital Forensics
- Scope-related Challenges to System Forensics
- Knowledge needed for Computer Forensics Analysis

Module 8 - Digital Forensics Methods and Labs

- Digital Forensics Methodologies
- Formal Forensics Approaches
- Documentation of Methodologies and Findings
- Evidence-handling Tasks

Module 9 - How to Set Up a Forensic Lab

- Equipment
- Security
- Standards and Frameworks
- Guidelines
- Case Studies
- Exercises

Module 10 - Common Forensics Software and Tools

- Open Source Tools
- Commercial Tools
- Case Studies
- Exercises

Module 11 - System Forensics, Investigation and Response

- Recovering data
- Undeleting data form OS's
- Windows Forensics
- Linux Forensics
- Recovering information from damages media
- Email Forensics
- Case Studies
- Exercises

Module 12 - Network Forensics, Investigation and Response

- Baselines and Anomalies
- Network Packet Analysis
- Network Traffic Analysis
- Router Forensics
- Firewall Forensics
- Case Studies
- Exercises

Module 13 - Mobile Forensics, Investigation and Response

- Cellular Device Concepts
- What evidence you can get from a cell phone
- Seizing evidence from a mobile device
- Case Studies
- Exercises

Module 14 - Cloud-based Systems Forensics and Investigation

- Cybercrime and the cloud
- Challenges faced by law enforcement and government agencies
- Cloud storage forensics framework
- Microsoft SkyDrive cloud storage forensics analysis
- Dropbox Analysis
- Google Drive Forensics Analysis
  - Google Drive Forensics Analysis Case Study:
    - Step 1: Commence (Scope)
    - Step 2: Preparation
    - Step 3: Evidence Source Identification and Preservation
    - Step 5: Collection
    - Step 6: Presentation
    - Step 7: Complete

Module 15 - Collecting, Seizing and Protecting Evidence

- Collecting evidence
- Handling evidence
- Storage formats
- Forensics imaging
- Case Studies
- Exercises

Module 16 - Incident Handling and Response

- Detecting incidents
- Collecting information
- Analyzing information
- Incident Response
- Incident Response Plan (IRP)
- Preserving Evidence
- Adding Forensics to Incident Response
- Digital Forensics Guidelines

Module 17 - Incident Management

- Presenting information to relevant parties
- Dealing with different cyber security incidents
- Triage to cyber security incidents
- Writing your first computer incident response plan
- Dealing with internal and external threats
- Communication to internal and external parties

Module 18 - Writing a Final Report

- The basics of report writing
- Writing an incident handling report
- Writing a digital forensics report
- Case Studies
- Exercises

Module 19 - Standards, Frameworks and Laws

- Putting Cybersecurity Standards and Frameworks in Context
- Commonly used frameworks and standards
- Constraints on standards and frameworks
- Laws and regulations affecting Digital Forensics
- Case Studies
- Exercises

Module 20 - Trends and Future Directions

- Security Orchestration and Automation
- Challenges of Incident Response in the digital world
- SIEM 2.0 (Next Generation)
- SOC 2.0 (Next Generation)

Exam

- 250 multiple choice questions.
- Six hours.

Certification

- **TS-College** Certified Cyber Security Operator (CCSO®)

Titans Security **College**