CTR-900 SOC Analyst

About this course

This is a 24-hour course that trains students on how to become a SOC Analyst which is the entry point into a SOC. It's intended to help working analysts and those hoping to enter the SOC security operations field.

By learning from some of the most seasoned educators in the business, participants in this training and certification program can obtain cutting-edge technical skills in high demand. This course begins with a review of the principles of SOC operations and progresses to include log management and correlation, SIEM implementation, advanced incident detection, and incident response. The applicant will also get experience managing different SOC procedures and working with the CSIRT as needed.

This program emphasizes the holistic approach to delivering elementary as well as advanced knowledge of how to identify and validate intrusion attempts. Through this, the candidate will learn to use SIEM solutions and predictive capabilities using threat intelligence. The program also introduces the practical aspect of SIEM using advanced and the most frequently used tools. The candidate will learn to perform enhanced threat detection using the predictive capabilities of Threat Intelligence.

Audience profile

The course is designed to help participants find better jobs by expanding their skill sets and preparing them to make significant contributions to a SOC team at higher levels of responsibility.

At course completion

After completing this course, students will be able to:

- Attempt the SOC Analyst exam. Upon successful completion of the exam, with a score of at least 70%, the candidate will be entitled to a certificate and membership privileges.
- Members are expected to adhere to recertification requirements through EC-Council's Continuing Education Requirements

Course details:

Module 1: Security Operations and Management

This module will teach students about security operations management and covers the entire system and infrastructure. It goes beyond threat analysis and risk management. You'll learn how companies invest in security operations management software that can work with optimized processes that are completely secure and, thus, provide better outcomes.

Module 2: Understanding Cyber Threats, IoCs, and Attack Methodology

This module will cover everything on cyber-attack that can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks. Cybercriminals use a variety of methods to launch a cyber-attack, including malware, phishing, ransomware, and denial of service, among other methods.

Module 3: Incidents, Events, and Logging
This module educates students on event history, simplifies security analysis, resource change tracking, and troubleshooting. Students will learn about events and logs management tools help analyze logs, monitor important events recorded in logs, and leverage them to identify and investigate security incidents.

Module 4: Incident Detection with Security Information and Event Management (SIEM)
This module teaches you about the process of identifying threats by actively monitoring assets and finding anomalous activity and how security information and event management (SIEM) is a security solution that helps organizations detect threats before they disrupt business.

Module 5: Enhanced Incident Detection with Threat Intelligence
Here, you will learn how threat intelligence feeds support early incident detection by helping teams classify high—risk activities and security incidents. This information is especially useful when integrated into an automated incident response pipeline because it helps predict the course of an attack.

Module 6: Incident Response
The student will learn about a set of information security policies and procedures that you can use to identify, contain, and eliminate cyberattacks.

Prerequisites:

- Entry Level exam (American test)
- The CSA program requires a candidate to have 1 year of work experience in the Network Admin/Security domain and should be able to provide proof of the same as validated through the application process unless the candidate attends official training.