

# ECCC-10 - CSA - CERTIFIED SOC ANALYST

Categoria: **EC-Council**

## INFORMAZIONI SUL CORSO



**Durata:**  
3 Giorni



**Categoria:**  
EC-Council



**Qualifica Istruttore:**  
Certified EC-Council  
Instructor



**Dedicato a:**  
Professionista IT



**Produttore:**  
EC-Council

## OBIETTIVI

Il programma del corso è stato concepito per gli analisti di livello I e II allo scopo di dar loro le competenze necessarie per effettuare operazioni di primo e secondo livello.

Si tratta di un corso intensivo di 3 giorni che copre a fondo i principi fondamentali delle operazioni SOC, della gestione e correlazione di log, dell'implementazione SIEM, della rilevazione avanzata di incidenti fino alla loro risposta.

Inoltre i partecipanti impareranno a gestire numerosi processi SOC e a collaborare con il CSIRT.

## PREREQUISITI

Il conseguimento preventivo delle certificazioni CND - Certified Network Defender e CEH - Certified Ethical Hacker è consigliato.

## CONTENUTI

Modulo 01: Security Operations and Management

Modulo 02: Understanding Cyber Threats, IoCs, and Attack Methodology

Modulo 03: Incidents, Events, and Logging

Modulo 04: Incident Detection with Security Information and Event Management (SIEM)

Modulo 05: Enhanced Incident Detection with Threat Intelligence

Modulo 06: Incident Response

## INFO

**Esame:** 312-39 - Certified SOC Analyst

**Materiale didattico:** Materiale didattico ufficiale EC-Council in formato digitale e comprensivo di voucher esame

**Costo materiale didattico:** incluso nel prezzo del corso a Calendario

**Natura del corso:** Operativo (previsti lab su PC)