**Iverson Associates Sdn Bhd (303330-M)**
Suite T113 – T114, 3rd Floor, Centrepoint, Lebuh Bandar Utama
Bandar Utama, 47800 Petaling Jaya, Selangor Darul Ehsan
Tel: 03-7726 2678 Fax: 03-7727 9737 Website: www.iverson.com.my



**Module Title : CERTIFIED SOC ANALYST (CSA)**
**Duration : 3 days**

## Overview

The Certified SOC Analyst (CSA) program is the first step to joining a security operations center (SOC). It is engineered for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entry-level and intermediate-level operations.

CSA is a training and credentialing program that helps the candidate acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team. Being an intense 3-day program, it thoroughly covers the fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response. Additionally, the candidate will learn to manage various SOC processes and collaborate with CSIRT at the time of need.

## Target Audience

- SOC Analysts (Tier I and Tier II)
- Network and Security Administrators, Network and Security Engineers, Network Defense Analyst, Network Defense Technicians, Network Security Specialist, Network Security Operator, and any security professional handling network security operations
- Cybersecurity Analyst
- Entry-level cybersecurity professionals
- Anyone who wants to become a SOC Analyst.

## Certification

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

## Exam Eligibility Requirement

The CSA program requires a candidate to have one 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.

## Course Outline

**Module 1 –** Security Operations and Management

**Module 2 –** Understanding Cyber Threats, IoCs, and Attack Methodology

**Module 3 –** Incidents, Events, and Logging

**Module 4 –** Incident Detection with Security Information and Event Management (SIEM)

**Module 5 –** Enhanced Incident Detection with Threat Intelligence

**Module 6 –** Incident Response