CSA Certified SOC Analyst

Why Learn CSA Certified SOC Analyst?

Certified SOC Analyst course is the initial step to joining a security operations center (SOC).

Its enables the candidate to acquire trending and in-demand technical skills through instruction by some of the most experienced instructors in the industry.

Audience Profile :

- 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.

Prerequisites:

- Anyone who wants to become a SOC Analyst.

Course Overview:

- The Certified SOC Analyst (CSA) Training Course 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 entrylevel and intermediate-level operations.
- Certified SOC Analyst (CSA) Training Course 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 Certified SOC Analyst (CSA) Training Course 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 Course, 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.
- As the security landscape is expanding, a SOC team offers high-quality IT-security services to detect potential cyber threats/attacks actively and quickly respond to security incidents. Organizations need skilled SOC Analysts who can serve as the front-line defenders, warning other professionals of emerging and present cyber threats.
- The lab-intensive SOC Analyst training course emphasizes the holistic approach to deliver elementary as well as advanced knowledge of how to identify and validate intrusion attempts.
- Through this SOC Analyst training course , the candidate will learn to use SIEM solutions and predictive capabilities using threat intelligence.
- The SOC Analyst training course 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.

CSA Certified SOC Analyst Outline:

- Module 1: Security Operations and Management
- Understand the SOC Fundamentals
- Discuss the Components of SOC: People, Processes and Technology
- Understand the Implementation of SOC
- Module 2: Understanding Cyber Threats, IoCs, and Attack Methodology
- Describe the term Cyber Threats and Attacks
- Understand the Network Level Attacks
- Understand the Host Level Attacks
- Understand the Application Level Attacks
- Understand the Indicators of Compromise (IoCs)
- Discuss the Attacker’s Hacking Methodology
- Module 3: Incidents, Events, and Logging U
- Understand the Fundamentals of Incidents, Events, and Logging
- Explain the Concepts of Local Logging
- Explain the Concepts of Centralized Logging
- Module 4: Incident Detection with Security Information and Event Management (SIEM)
- Understand the Basic Concepts of Security Information and Event Management (SIEM)
- Discuss the Different SIEM Solutions
- Understand the SIEM Deployment
- Learn Different Use Case Examples for Application Level Incident Detection
- Learn Different Use Case Examples for Insider Incident Detection
- Learn Different Use Case Examples for Network Level Incident Detection
- Learn Different Use Case Examples for Host Level Incident Detection
- Learn Different Use Case Examples for Compliance
- Understand the Concept of Handling Alert Triaging and Analysis
- Module 5: Enhanced Incident Detection with Threat Intelligence
- Learn Fundamental Concepts on Threat Intelligence
- Learn Different Types of Threat Intelligence
- Understand How Threat Intelligence Strategy is Developed
- Learn Different Threat Intelligence Sources from which Intelligence can be Obtained
- Learn Different Threat Intelligence Platform (TIP)
- Understand the Need of Threat Intelligence-driven SOC
- Module 6: Incident Response
- Understand the Fundamental Concepts of Incident Response
- Learn Various Phases in Incident Response Process
- Learn How to Respond to Network Security Incidents
- Learn How to Respond to Application Security Incidents
- Learn How to Respond to Email Security Incidents
- Learn How to Respond to Insider Incidents
- Learn How to Respond to Malware Incidents

Training Solutions:

√ Offline Classroom Instructor-Led Training in our labs or onsite Locations.

√ Virtual Instructor-Led Training Via Virtual Video Conferencing Tools.

Why Learners Prefer CLS as their Training Services provider ?

■ Premuim Training Services Accredited from Global Technology Vendors.

■ Best Rated Experts & Certified Trainers in Egypt.

■ Official Training Hours, Practice Labs, Hands-on Learning.

■ CLS Training Classrooms are designed with High Edge PCs and Training Facilities.

■ Return on Training Investment is Guaranteed to boost performance.

CLS Learning Solutions
Training businesses and people Since 1995