Certified SOC Analyst

Course Duration: 24 Hrs. **Course code: 312-39**

Course Overview

A Certified SOC Analyst (CSA) course prepares individuals for roles in Security Operations Centers (SOCs) by equipping them with the skills to identify, analyze, and respond to security incidents, covering SOC fundamentals, incident detection, and response.

What you'll learn?

A Certified SOC Analyst course equips you with the skills to understand, detect, and respond to security threats within a Security Operations Center (SOC), covering SOC operations, cyber threats, incident detection with SIEM, threat intelligence, and incident response.

Target Audience

The target audience for a Certified SOC Analyst (CSA) course typically includes aspiring and current cybersecurity professionals, IT professionals seeking SOC expertise, incident response team members, and those looking to enhance their cybersecurity skills and incident handling abilities.

Pre-Requisites

To pursue a Certified SOC Analyst (CSA) course, you'll typically need a foundational understanding of networking, security principles, and IT concepts, along with some relevant experience or a related educational background.

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

Course content

Module 01: Security Operations and Management

A. Security Management
B. Security Operations
C. Security Operations Center (SOC)
D. Need of SOC
E. SOC Capabilities
F. SOC Operations
G. SOC Workflow
H. Components of SOC: People, Process and Technology
I. Types of SOC Models
J. SOC Key Performance Indicators (KPI) and Metrics
K. Challenges in Implementation of SOC
L. Best Practices for Running SOC
M. SOC vs NOC

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

A. Cyber Threats
B. Intent-Motive-Goal
C. Tactics-Techniques-Procedures (TTPs)
D. Opportunity-Vulnerability-Weakness
E. Network Level Attacks
F. Host Level Attacks
G. Application-Level Attacks
H. Email Security Threats
I. Understanding Indicators of Compromise (IoCs)
J. Understanding Attacker's Hacking Methodology

Module 03: Incidents, Events, and Logging

A. Incident
B. Event
C. Log

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

D. Typical Log Sources
E. Need of Log
F. Logging Requirements
G. Typical Log Format
H. Logging Approaches
I. Centralized Logging

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

A. Security Information and Event Management (SIEM)
B. Security Analytics
C. Need of SIEM
D. SIEM Architecture and Its Components
E. SIEM Solutions
F. SIEM Deployment
G. Incident Detection with SIEM

Module 05: Enhanced Incident Detection with Threat Intelligence

A. Understanding Cyber Threat Intelligence
B. Why Threat Intelligence-driven SOC?

Module 06: Incident Response

A. Incident Response
B. Incident Response Team (IRT)
C. Where Does IRT Fits in the Organization?
D. SOC and IRT Collaboration
E. Incident Response (IR) Process Overview

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

Exam Preference

Exam Code	312-39
Length Of Test	180 Minutes
Number Of Questions	100 MCQ.