**SOC-CMM Certified Assessor**

## Overview

The SOC-CMM Certified Assessor (SOC-CA) course is designed to equip professionals with the knowledge and skills required to assess and enhance the maturity of Security Operations Centers (SOCs) using the SOC-CMM framework. This comprehensive training provides an in-depth understanding of SOC models, operational challenges, and evaluation methodologies. Participants will learn how to conduct SOC maturity assessments across key domains, including business alignment, people, processes, technology, and services. The course also covers the SOC Target Operating Model (SOCTOM), offering insights into optimizing SOC capabilities and addressing common operational challenges. Through practical exercises and hands-on demonstrations, attendees will gain the expertise needed to apply SOC-CMM in real-world scenarios, ensuring continuous improvement and alignment with organizational security goals.

## Intended Audience

This course is ideal for SOC managers, cybersecurity consultants, auditors, and security professionals responsible for assessing and improving SOC operations. It is particularly beneficial for those involved in SOC governance, security monitoring, incident response, and compliance. Individuals seeking to enhance their understanding of SOC maturity assessments and gain practical experience with the SOC-CMM tool will find this training highly valuable. Whether working within an internal SOC, a managed security services provider (MSSP), or a regulatory body, participants will leave with actionable insights to drive SOC efficiency and effectiveness.

## Day 1:

1. **Introduction to Security Operations Centers (SOCs)**
    - Overview of Security Operations
    - Different SOC models and types
    - Understanding Hybrid SOCs
    - Distinguishing SOCs from CSIRTs
2. **SOC-CMM Framework**
    - Goals and principles of SOC-CMM
    - Versioning and updates
    - Detailed breakdown of the SOC-CMM model
    - Exploring capability and maturity levels
    - Application of SOC-CMM for CERTs
    - Understanding the limitations of SOC-CMM
3. **Preparing for a SOC-CMM Assessment**
    - Defining the purpose and scope of the assessment

- Selecting the appropriate assessment type
- Strategies for effective information collection
- Resource planning and allocation
- Setting clear report expectations

**Day 2:**

1. **Conducting the SOC-CMM Assessment**
   - Utilizing the SOC-CMM tool effectively
   - Assessing the Business domain
   - Evaluating the People domain
   - Analyzing the Process domain
   - Reviewing the Technology domain
   - Scrutinizing the Service domain
2. **Analysis and Reporting**
   - Interpreting assessment results
   - Conducting a thorough analysis
   - Compiling a comprehensive assessment report
3. **SOC Target Operating Model (SOCTOM)**
   - Components of SOCTOM
   - Defining and implementing the SOCTOM
   - Utilizing the SOCTOM tool
   - Understanding the SOCTOM process
4. **Addressing Common Challenges in Modern SOCs**
   - Business-related challenges
   - Employee and staffing challenges
   - Process optimization challenges
   - Technological challenges and solutions