Certified Threat Intelligence Analyst

Course Duration: 40 Hrs. **Course code: 312-85**

Course Overview

CTIA is a comprehensive specialist- level program that teaches a structured approach for building effective threat intelligence.

A program developed by threat intelligence experts from all over the world that is constantly updated to ensure that the students are exposed to the latest advances in the field of Threat Intelligence.

What you'll learn?

- **Understanding Threat Intelligence:**
  Learn the fundamentals of threat intelligence, its importance in risk management, SIEM, and incident response.
- **Cyber Threat Landscape:**
  Gain knowledge of various cyber threats, threat actors, and their objectives.
- **Threat Intelligence Lifecycle:**
  Understand the stages of the threat intelligence lifecycle, including requirements, planning, direction, and review.
- **Cyber Kill Chain Methodology:**
  Learn the Cyber Kill Chain methodology and its application in threat analysis.

Target Audience

The course is designed for individuals working in various cybersecurity roles, including:

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

- **Threat Intelligence Analysts:**
  Those who specialize in gathering, analyzing, and disseminating threat intelligence.
- **Security Analysts:**
  Individuals involved in analyzing security incidents and threats.
- **Security Operations Center (SOC) Staff:**
  Professionals working in security operations and incident response.
- **Incident Response Team Members:**
  Those who handle security incidents and coordinate response efforts.

Pre-Requisites

To successfully undertake the Certified Threat Intelligence Analyst (CTIA) course, you should have a basic understanding of cybersecurity concepts and terminology, familiarity with information security principles, and some experience with incident response or security operations, though not mandatory.

Course content

Module 01: Introduction to Threat Intelligence

A. Understanding Intelligence
B. Understanding Cyber Threat Intelligence
C. Overview of Threat Intelligence Lifecycle and Frameworks

Module 02: Cyber Threats and Kill Chain Methodology

A. Understanding Cyber Threats
B. Understanding Advanced Persistent Threats (APTs)
C. Understanding Cyber Kill Chain
D. Understanding Indicators of Compromise (IoCs)

Module 03: Requirements, Planning, Direction, and Review

A. Understanding Organization's Current Threat Landscape
B. Understanding Requirements Analysis
C. Planning Threat Intelligence Program

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

D. Establishing Management Support
E. Building a Threat Intelligence Team
F. Overview of Threat Intelligence Sharing
G. Reviewing Threat Intelligence Program

Module 04: Data Collection and Processing

A. Overview of Threat Intelligence Data Collection
B. Overview of Threat Intelligence Collection Management
C. Overview of Threat Intelligence Feeds and Sources
D. Understanding Threat Intelligence Data Collection and Acquisition
E. Understanding Bulk Data Collection
F. Understanding Data Processing and Exploitation

Module 05: Data Analysis

A. Overview of Data Analysis
B. Understanding Data Analysis Techniques
C. Overview of Threat Analysis
D. Understanding Threat Analysis Process
E. Overview of Fine-Tuning Threat Analysis
F. Understanding Threat Intelligence Evaluation
G. Creating Runbooks and Knowledge Base
H. Overview of Threat Intelligence Tools

Module 06: Intelligence Reporting and Dissemination

A. Overview of Threat Intelligence Reports
B. Introduction to Dissemination
C. Participating in Sharing Relationships
D. Overview of Sharing Threat Intelligence
E. Overview of Delivery Mechanisms
F. Understanding Threat Intelligence Sharing Platforms
G. Overview of Intelligence Sharing Acts and Regulations
H. Overview of Threat Intelligence Integration

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

Exam Preference

Exam Code	312-85
Length Of Test	120 Minutes
Number Of Questions	50
Passing Score	70%