Certified Cyber Threat Analyst (CCTA)

Course Duration: 32 Hours **Course code: CCTA**

1. Course Overview

The Certified Cyber Threat Analyst (CCTA) course equips cybersecurity professionals with the knowledge and skills to detect, analyze, and respond to cyber threats in real-time. This training emphasizes threat intelligence, malware analysis, incident response, network forensics, and vulnerability management. Learners will work with advanced security tools and frameworks to proactively defend organizations against cyberattacks. The course is designed to bridge the gap between theoretical security concepts and practical threat analysis, preparing analysts for roles in Security Operations Centers (SOCs), threat hunting teams, and incident response units.

2. What you'll learn?

By the end of the course, participants will be able to:

- Understand the role of a Cyber Threat Analyst in modern cybersecurity operations.
- Apply cyber kill chain and MITRE ATT&CK framework for threat modeling.
- Conduct threat intelligence gathering and analysis.
- Perform malware analysis using sandboxing and reverse engineering basics.
- Execute network forensics and packet analysis to detect intrusions.
- Identify, analyze, and respond to phishing, ransomware, and advanced persistent threats (APTs).
- Use SIEM tools for monitoring and correlation of security events.
- Perform threat hunting to proactively detect suspicious behavior.
- Develop incident response playbooks and conduct digital forensics.
- Apply reporting and communication techniques for threat intelligence sharing.

3. Target Audience

- SOC Analysts (Level 1–3)
- Cybersecurity Analysts and Engineers
- Incident Response Team Members
- Network Security Specialists
- IT Professionals aspiring to move into threat intelligence and analysis roles

4. Pre-Requisites

- Basic knowledge of networking, operating systems, and security fundamentals.
- Familiarity with cybersecurity tools and monitoring concepts.
- Prior experience in IT security, system administration, or network administration is recommended.

5. Course content

Module 1: Introduction to Cyber Threat Analysis

Role of a Cyber Threat Analyst

Cyber threat landscape and attack vectors

Threat actor motivations and tactics

Module 2: Cyber Threat Intelligence (CTI)

Threat intelligence lifecycle

Open-source intelligence (OSINT) tools and techniques

Integrating CTI into security operations

Module 3: Cyber Kill Chain & MITRE ATT&CK Framework

Phases of the cyber kill chain

Mapping threats to MITRE ATT&CK

Using frameworks for threat modeling

Module 4: Malware Analysis Fundamentals

Types of malware and attack delivery methods

Static and dynamic analysis

Using sandboxes for malware testing

Module 5: Network Forensics & Intrusion Detection

Packet capture and analysis with Wireshark

Identifying anomalies in network traffic

Detecting lateral movement and data exfiltration

Module 6: Threat Hunting

Proactive vs. reactive security

Hypothesis-driven threat hunting

Using SIEM and EDR tools for detection

Module 7: Security Monitoring and SIEM

Log collection and correlation

Configuring alerts and dashboards

Use cases for detecting advanced threats

Module 8: Incident Response & Digital Forensics

Incident response lifecycle (Preparation, Detection, Analysis, Containment, Eradication, Recovery)

Forensic imaging and evidence handling

Developing playbooks and automation in response

Module 9: Vulnerability & Risk Management

Identifying and prioritizing vulnerabilities

Threat and risk correlation

Patch and remediation strategies

Module 10: Reporting & Communication
Writing effective threat intelligence reports
Sharing intelligence across teams and organizations
Collaboration with CERTs and ISACs

Module 11: Capstone Project / Lab
Hands-on threat hunting exercise
Malware analysis in sandbox environment
Incident response simulation and reporting

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