Syntho Quest

CERTIFIED SOC ANALYST

COURSE

Prepared By (CTO) SYNTHOQUEST

45 Days Duration

Duration: 45 days × 2 hrs/day = 90 hrs

Goal: Equip professionals with the knowledge and skills to monitor, detect, analyze, and respond to cybersecurity incidents within a Security Operations Center (SOC).

Core Domains

1. **Introduction to SOC & Cybersecurity (10%)**
   - SOC roles and responsibilities
   - Cybersecurity fundamentals: threats, vulnerabilities, and attack vectors
   - SOC workflow, incident response lifecycle
2. **Network Fundamentals & Monitoring (15%)**
   - TCP/IP, OSI model, protocols, ports, and services
   - Network traffic monitoring and analysis
   - SIEM overview: log sources, collection, and correlation
3. **Security Information & Event Management (SIEM) (20%)**
   - SIEM setup, log aggregation, parsing, normalization
   - Event correlation, alert generation, and dashboards
   - Using SIEM tools (Splunk, ELK, QRadar)
4. **Threat Intelligence & Indicators of Compromise (IoCs) (15%)**
   - Threat intelligence sources and platforms
   - Collecting and analyzing IoCs
   - Mapping IoCs to MITRE ATT&CK framework
5. **Incident Detection & Response (20%)**
   - Alert triage and prioritization
   - Investigation techniques for malware, phishing, and network attacks
   - Containment, eradication, and recovery strategies
6. **Endpoint & Log Analysis (10%)**
   - Endpoint monitoring and forensic basics
   - Log analysis: Windows, Linux, network devices, and applications
   - Identifying anomalies and suspicious activity
7. **Reporting & Documentation (10%)**
   - Incident documentation templates and executive reports
   - Metrics, KPIs, and SOC performance tracking
   - Lessons learned and continuous improvement

Business Associate: vivek
Email: contact@synthoquest.com
Mobile: +91-8333801638 (whats app)