Syntho Quest

CERTIFIED INCIDENT HANDLER

COURSE

Prepared By (CTO) SYNTHOQUEST

45 Days Duration

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

Goal: Equip professionals to identify, respond to, and manage cybersecurity incidents effectively across networks, systems, and applications.

Core Domains

1. **Introduction to Incident Handling (10%)**
   - Cybersecurity incidents overview
   - Types of attacks: malware, ransomware, phishing, DoS/DDoS
   - Incident handling life cycle & framework
2. **Incident Handling & Response Planning (20%)**
   - Policies & standard operating procedures
   - Roles and responsibilities (CSIRT, SOC, stakeholders)
   - Preparation & playbook development
3. **Detection & Analysis (20%)**
   - Event collection: SIEM, logs, alerts
   - Traffic & packet analysis
   - Identifying indicators of compromise (IoCs) and TTPs
   - Malware analysis basics
4. **Containment, Eradication & Recovery (20%)**
   - Short-term vs long-term containment
   - Malware removal, system hardening, patching
   - Recovery planning and business continuity integration
5. **Forensics & Evidence Management (15%)**
   - Disk, memory, and network forensics
   - Chain of custody and evidence preservation
   - File integrity monitoring & forensic tools
6. **Communication & Reporting (15%)**
   - Incident documentation templates
   - Executive and technical reporting
   - Lessons learned, post-incident review, metrics & KPIs

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