Syntho Quest

CERTIFIED MALWARE ANALYSIS PROFESSIONAL

COURSE

Prepared By (CTO) SYNTHOQUEST

45 Days Duration

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

Goal: Equip professionals with the skills to detect, analyze, and mitigate malware threats across systems and networks.

Core Domains

1. **Introduction to Malware (10%)**
   - Types of malware: viruses, worms, trojans, ransomware, spyware, rootkits
   - Malware lifecycle and attack vectors
   - Threat landscape & motivations of attackers
2. **Malware Analysis Fundamentals (15%)**
   - Malware analysis methodology: static, dynamic, memory, and hybrid analysis
   - Setting up safe lab environments (VMs, sandboxes)
   - Malware classification & identification
3. **Static Analysis (15%)**
   - Examining file properties, headers, strings, and metadata
   - Binary analysis, reverse engineering basics
   - Identifying obfuscation, packers, and encryption
4. **Dynamic Analysis (20%)**
   - Running malware in isolated environments
   - Monitoring behavior: file system, registry, processes, network activity
   - Capturing indicators of compromise (IoCs)
5. **Memory & Advanced Analysis (15%)**
   - Memory forensics: Volatility, RAM dumps
   - Hooking & API monitoring
   - Rootkit detection & analysis
6. **Malware Mitigation & Threat Intelligence (10%)**
   - Signature-based vs behavior-based detection
   - Updating AV/EDR rules, sandboxing, network containment
   - Malware threat intelligence integration into SOC
7. **Reverse Engineering & Exploit Analysis (10%)**
   - Disassembly & decompilation basics
   - Identifying exploits in malware
   - Safe reverse engineering practices
8. **Reporting & Documentation (5%)**
   - Malware analysis report format: IoCs, behavior, mitigations
   - Executive summary vs technical details
   - Threat advisory preparation

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