CREST Registered Intrusion Analyst (CRIA)

Module 1: Soft Skills and Incident Handling

- Incident Chronology
- Record Keeping, Interim Reporting & Final Results

Module 2: Core Technical Skills

- IP Protocols
- Common Classes of Tools
- OS Fingerprinting
- Application Fingerprinting
- Network Access Control Analysis
- File System Permissions
- Host Analysis Techniques

Module 3: Background Information Gathering & Open Source

- Domain Name Server (DNS)

Module 4: Network Intrusion Analysis

- Network Traffic Capture
- Data Sources and Network Log Sources
- Network Configuration Security Issues
- Beaconing
- Command and Control Channels
- Exfiltration of Data
- Incoming Attacks
- Reconnaissance
- Internal Spread and Privilege Escalation
- False Positive Acknowledgement

Module 5: Analysing Host Intrusions

- Windows File Structures
- Application File Structures

- Windows Registry Essentials
- Identifying Suspect Files
- Infection vectors
- Live Malware Analysis

Module 6: Reverse Engineering Malware

- Functionality Identification
- Processor Architectures
- Windows Executable File Formats
- Behavioural Analysis

Module 7: CRIA Exam Preparation & Mock Exam

- CRIA - Examination Guidance
- CRIA - Practice Exam