RCCI: Rocheston Certified Cybercrime Investigator

Course Code: RCCI
Duration: 5 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

Rocheston's courseware is designed to ensure industry relevance. SMEs deliver the course content in a five-day learning capsule. Cybercrime will be worth 411M USD in a few years. Its global nature will necessitate an evolving standard to fight it. Threat neutralization will require best practices and protocol that are common across borders. This is where Rocheston's RCCI steps in.

SKILLS COVERED

- Awareness about Digital Forensics
- Forensic Analysis
- Setting up Digital Forensic Capabilities
- Preparing Organizations for Cyber Security Incidents
- Conducting Digital Investigations
- Performing the Forensic Process
- Collecting, Examining and Analyzing Files
- Investigative Reconstruction with Digital Evidence
- Using Digital Evidence from Windows Systems
- Using Digital Evidence from Macintosh Systems
- Using Digital Evidence from UNIX Systems
- Intrusion Analysis
- Network Forensics
- Network Intrusion Detection and Analysis
- Mobile Forensics Investigation
- Email Forensics Investigation
- Steganalysis
- NIST Projects for Digital Forensics
- Cyberforensics Investigation Reporting
- Cybercrime Laws (USA & Europe)

WHO SHOULD ATTEND?

- CEOs, COOs, CFOs, CTOs and CIOs
- Entrepreneurs
- Students of cybercrime
- Students of cyber investigation
- Students of law enforcement methodology
- RCCIs can be game changers both in corporate and other environments.

PREREQUISITES

There are no prerequisites required to attend this course.

MODULES

Module 1: Awareness about Digital Forensics

- What is Digital Evidence?
- Digital Evidence: Past, Present and Future
- Principles of Digital Evidence
- Digital Forensic Results
- Digital Forensics Evidence Collection Tools

Module 2: Forensic Analysis

- Forensic Artifact Handling
- Malware and Implant Analysis
- Forensic Artifact Analysis
- Phishing Detection and Prevention
- Insider Threat Detection Using Machine Learning
- Defining Levels of Certainty

Module 3: Setting up Digital Forensic Capabilities

- Defining Roles and Responsibilities
- Cybercrime Investigation Infrastructure, Tools, Skills
- Supporting Forensics in the Information System Life Cycle
- Setting Up Digital Forensics Lab: Global Guidelines

Module 4: Preparing Organizations for Cybersecurity Incidents

- Conducting critical assessment of organizations
- Carrying out a cybersecurity threat analysis
- Digital Investigation Process Models
- Understanding Roles and Responsibilities
- Understanding Threshold Considerations
- Assessing Cybersecurity Incident Alert Situation

Module 5: Conducting Digital Investigations

- Identifying Cyber Security Incident
- Applying Investigation Models
- Formation and Evaluation of Hypotheses
- Creating a plan of action
- Recognizing sources of digital evidence
- Conducting Examination for Extracting and Viewing Information
- Conducting Forensic Analysis
- Preparing report

Module 6: Performing the Forensic Process

- Identifying Source of Data
- Identifying Possible Sources of Data
- Developing Plan to Acquire Data

Module 7: Collecting, Examining and Analyzing Files

- Different media types that are used to store files
- Maintaining File Systems
- Collecting and Maintaining Media Files
- Examining, Locating and Extracting Data Files
- Using Forensic Toolkit

Module 8: Investigative Reconstruction with Digital Evidence

- What is Investigative Reconstruction?
- Equivocal Forensic Analysis
- Victimology
- Risk Assessments

Module 9: Using Digital Evidence from Windows Systems

- Understanding Windows File systems
- Data Recovery Process
- Windows-based Recovery Tools
- Picking up Information from Internet

Module 10: Using Digital Evidence from Macintosh Systems

- Understanding Macintosh File systems
- Data Recovery Process
- Macintosh-based Recovery Tools
- Picking up Information from Internet

Module 11: Using Digital Evidence from UNIX Systems

- Understanding UNIX File systems
- Linux-based acquisition and examination systems
- File Carving with UNIX
- Log Files Configurations
- Password Protection and Encryption
- Picking up Information from Internet

Module 12: Intrusion Analysis

- Analyzing intrusions
- Methods of conducting intrusion analysis
- Best intrusion detection system tools

Module 13: Network Forensics

- Types of Network Attacks
- Network Forensics Investigation Methodology (OSCAR)
- Network-based Evidence Acquisition
- Network Forensic Analysis Tools

Module 14: Network Intrusion Detection and Analysis

- NIDS/NIPS: Types & Functionality
- Different Modes of Detection
- Network Tunneling: Covert Tunneling Strategies
- Network Worm Propagation Investigation

Module 15: Mobile Forensics Investigation

- Introduction to Mobile Forensics
- Gathering Forensic Information from Android Devices
- Decoding and Extracting Information from iOS Devices
- Mobile Forensic Software Tools

Module 16: Email Forensics Investigation

- Email Forensics Investigation Techniques
- Email Header Analysis
- Email Recovery

Module 17: Steganalysis

- Understanding How Steganography Works
- Steganography Techniques
- Steganalysis in Digital Forensics Investigation
- Tools Used by Steganalyst
- Detecting Hidden Information (Image & Audio Files)

Module 18: NIST Projects for Digital Forensics

- National Software Reference Library (NSRL)
- Computer Forensic Tool Testing (CFTT)
- Computer Forensic Reference Data Sets (CFReDS)
- Computer Security Incident Response Team (CSIRT) with SOAR

Module 19: Cyber Forensics Investigation Reporting

- Importance of Documenting Cyber Forensics Investigation Results
- Standards for Reporting Digital Evidence Findings
- Investigation Examiner's Report
- Analysis of Cyber Forensics Reporting

Module 20: Cybercrime Laws (USA & Europe)

- Federal Cybercrime Law
- State Cybercrime Law
- Fifth Amendment and Encryption
- Council of Europe Convention on Cybercrime and Protocol
- Copyright Infringement and Cyberbullying

END OF PAGE