Real Time College

Course: Forensics Investigation & Incident Response

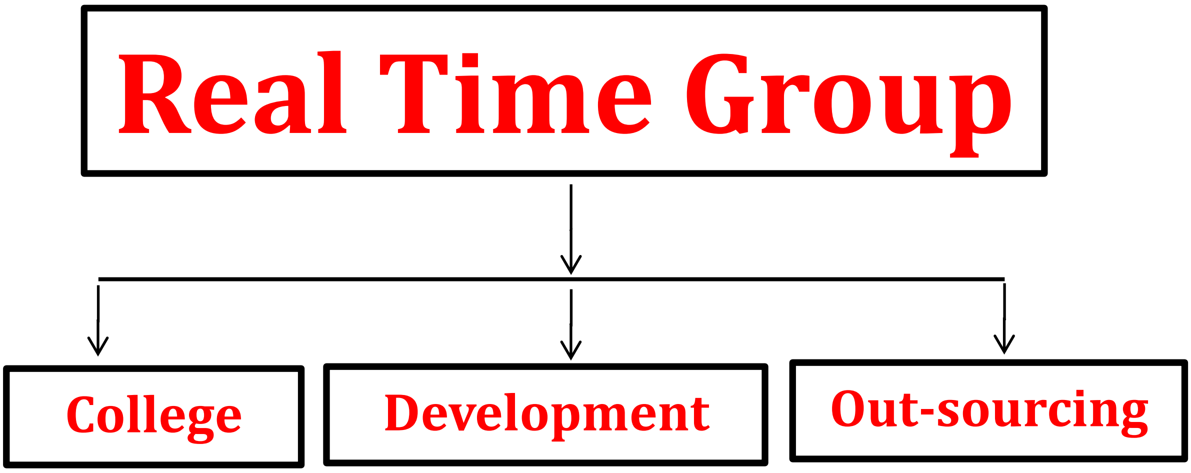
Duration: 50 Hours

Hands-On-Training: 50%

Real Time Group is a multi-disciplinary dynamic and innovative Real-Time O.S. and Software Solutions Center, established in 2007.

Providing Software, Security and Embedded Linux solutions, professional services and consulting, end-to-end flexible system infrastructure, outsourcing, integration and training services for Hardware, Software and RT-OS \ Embedded Systems.

The company is divided into the following three Divisions:



Real Time Group

College

Development

Out-sourcing

rt-ed.co.il rt-dev.com rt-hr.co.il

Training Division:

Professional Training Services for Software, Cyber Security, IT, RT-OS and Embedded systems industries.

We provide the knowledge and experience needed to enable professional engineers to Develop, Integrate and Automate Hardware, Software and Networking Projects.

To ensure experience, all courses are practical – Hands-On-Training.
The latest Development, Cyber Security, IT and Automation equipment which are adopted by the industry are used.

All students are supplied with necessary equipment (i.e. software license, AWS Account, etc) for Class -work \ Home-work and course projects.

Course Overview:

This **Forensics Investigation & Incident Response** Course is part of RT-Group's Cyber-Security Complete Track hand-on-training course, which provides the most complete and comprehensive Cyber Security Course.

This course explores the core principles of hands-on incident response (IR).
You will learn the major symptoms, how to prepare and set up security operations, defend against threats, actions needed to be taken when incidents occur, forensics techniques for incident handling, detection of attacks on networks, websites, and applications, Hands-on practical approaches for incident handling.

Workshops comprise approximately 50% of class time and are based around carefully designed exercises to reinforce and challenge the extent of learning.

Who should attend:

- Student with no experience who wish to learn Cyber Security – **must first pass the Cyber Fundamentals Exam\Course**.
- Candidates seeking to join **SOC teams** and specialize in forensics and cyber incident investigation.
- System\Linux Administrators wishing to upgrade their knowledge in Cyber Security.
- Architects \ Team Leaders \ Engineers \ Programmers who wish to participate in Cyber Security projects.

Prerequisite:

- Knowledge or experience in Networking is needed
- A medium level of computer literacy is expected, using a PC running Windows.
- Experience implementing scripts - Advantage.
- Experience in Linux or UNIX is necessary.

Forensics Investigation & Incident Response

1. **Introduction to Incident Response**
    a. What Is a Computer Security Incident?
    b. What Are the Goals of Incident Response?
    c. The Incident Response Process
    d. Incident response phases

2. **Pre-Incident Preparation**
    a. Preparing the Organization for Incident Response
    b. Identifying Risk
    c. Policies That Promote a Successful IR
    d. Global Infrastructure Issues
    e. Preparing the Infrastructure for Incident Response
    f. Computing Device Configuration and Network Configuration

3. **Incident Detection and Characterization**
    a. Discovering the Scope of the Incident
    b. Gathering and Reviewing Preliminary Evidence
    c. Determining a Course of Action
    d. Automated Clearing House (ACH) Fraud Scenario

4. **Live Data Collection**
    a. When to Perform a Live Response
    b. Live Response Tools
    c. Prebuilt Toolkits
    d. Memory Collection
    e. Live Data Collection on Microsoft Windows Systems
    f. Live Data Collection on Unix-Based Systems
    g. Live Response Toolkits

5. **Network Data Analysis**
    a. Network Monitoring
    b. Event-Based Alert Monitoring
    c. Header and Full Packet Logging
    d. Statistical Modeling
    e. Deploying Network Sensors
    f. Network Analysis Tools