CREST Practitioner Intrusion Analyst Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Delegates are provided with a Pearson Vue exam voucher for the CPIA examination as part of the course fee. This course prepares the student for a career in Incident Response and provides all of the tools and teaches the techniques needed by a practicing professional. This is the first cross discipline course of its' kind that covers the essential knowledge and skills needed for intrusion detection, incident handling, computer/network forensics and malware reverse engineering.

This course raises the bar and sets a new security baseline for aspiring Intrusion Analysis and Digital Forensics professionals. Every team member should take this course before embarking upon their very own, more specialised, career path.

You will learn how to detect an attack, how to handle it, how to trace and acquire the evidence, investigate, analyse and re-construct the incident. We then lay the groundwork for malware analysis by presenting the key tools and techniques malware analysts use to examine malicious programs. Quizzes and tests throughout, with feedback, re-enforce the knowledge and prepare you for the CPIA multiple choice exam.

Following this course a student may challenge the CREST core skills exam resulting in the CREST Practitioner Intrusion Analyst (CPIA) professional qualification, which is a pre-requisite for the CREST Registered Intrusion Analyst (CRIA) professional qualification. The CRIA exam can be challenged later, once more experience has been gained in real life scenarios.

Prerequisites

A good appreciation of the technical aspects of ICT and one year’s experience in network / server technical administration / operations. SEC-100 Security Essentials is reccomended.

Target Audience

- Aspiring information security personnel who wish to be part of an incident response team
- Existing practitioners wishing to become CREST Registered
- System administrators who are responding to attacks
- Incident handlers who wish to expand their knowledge into Digital Forensics
- Government departments who wish to raise and baseline skills across all security teams
- Law enforcement officers or detectives who want to expand their investigative skills
- Information security managers who would like to brush up on the latest techniques and processes in order to understand information security implications
- Anyone meeting the pre-requisites who is considering a career in Intrusion Analysis or Digital Forensics

CREST Practitioner Intrusion Analyst Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

Delegates will learn how to:

- Detect threats both before and after an attack occurs
- Apply advanced techniques to handle cyber-attacks in real time
- Hunt, trace, detect, and acquire evidence during and after incidents
- Conduct forensic investigation, investigate, analysis, and attack reconstruction
- Apply tools and techniques to examine network traffic, to discover anomalies
- Gain familiarity with malware behaviours, anti-forensics detection
- Prepare for the CREST Practitioner Intrusion Analyst (CPIA) exam