CERTIFIED PROFESSIONAL FORENSIC ANALYST (CPFA) TRAINING

A 12 Hours Forensics Analyst Training

Batch 1: Asia & Middle East

Dates : 4 – 6, April 2022
Time : 6 00 AM – 10 00 AM GMT
Mode : Online

Batch 2: Americas & Europe

Dates : 11 – 13, April 2022
Time : 2 00 PM – 6 00 PM GMT
Mode : Online

Fees:

Regular Participant – USD 150   ISACA & ISC2 Members – USD 120

Introduction

Cyber security threats continue to grow in volume and sophistication. While organizations are adopting the Work from home culture and getting adapted to the new normal, the WFH has significantly increased the attack surface which attackers are taking advantage of to target organizations.

Recently, many organizations have been targeted for ransomware attacks and data breaches, which have significantly impacted their businesses. In such circumstance's organizations need to adopt practices that allow them to rapidly identify, respond to, and mitigate these types of incidents while becoming more resilient and protecting against future incidents.

Whether your data has been compromised by a cyber-attack or your files encrypted by a cyber-crime like ransomware, it is important to know how the incident happened in your network, how to contain the incident, how to reduce the cost of the incident and at the same time how to quickly recover from the incident. Organizations also need to conduct post-incident analysis and forensics analysis to gather digital evidence which can be held in the court of law to bring the attackers to justice.

Importance Of Incident Response & Digital Forensics

Protecting your data from falling in the wrong hands or being held for ransom, protecting your reputation, customer's trust & loyalty, protecting your revenue and assisting law enforcement agencies are some critical reasons why organizations need to conduct forensic analysis and have a strong incident response plan today.

Incident response strategies and plans layout what defines a breach, the roles and responsibilities of the CSIRT (Cyber Security Incident Response) team, tools for managing a breach, steps that will need to be taken to address a security incident, how the incident will be investigated and communicated, and the notification requirements following a data breach.

"Remember….. you are the Centre of Security"

Why CPFA ?

The term cyber-crime no longer refers only to hackers and other external attackers. Almost all cases of financial fraud or employee misuse involves a very strong element of computer-based evidence.

The Certified Professional Forensics Analyst (CPFA) training is focused on comprehensive coverage of all aspects of digital forensics and incident response. It is designed to ensure that all aspects have a real-life scenario-based approach explaining start to end of digital forensics investigation, incident detection and response.

Objectives

- What should one do when there is a suspicion of a computer-based crime?
- What tools and techniques are most likely to yield the right set of clues?
- What is the procedure to deal with incident response and remediation?
- How should the investigation be carried out such that it can be presented in a court of law?

This Course Is Best For :

- Chief Security Officers, Chief Technology Officers, Chief Information Officers.
- Security practitioners and managers.
- Auditors and Fraud Examiners.
- Anyone interested in computer forensics and cyber-crime investigations.

The CPFA program is a scenario based training experience with case studies to explain the digital forensics and incident response process in much detail.

In line with these objectives, we are pleased to announce a 3-day 4-hours online training on "Certified Professional Forensics Analyst (CPFA)

"Remember….. you are the Centre of Security"

Session 1: Introduction to DFIR

- Digital Forensics Introduction
  - Digital Evidence
  - Forensic Process
  - Approaching Crime Scenes
  - Chain of Custody
- Incident Response Introduction
  - Important Case Studies
  - Getting your Incident Response Right
  - Incident Response Plan
  - Attacker Frameworks

Session 2: Endpoint Forensics

- Live Forensics
  - Performing Memory Forensics
  - Windows Live Forensics
  - Linux Live Forensics
- Log Analysis
  - Analysis of OS Logs

Session 3: Disk and OS Artifact Analysis

- Disk Forensics
  - Disk Image Acquisition
  - Disk Image Analysis
  - Windows File Systems
  - USB Forensics
- Windows Artifact Analysis
  - Windows Registry
  - Windows Shortcuts
  - Evidence of Execution

"Remember….. you are the Centre of Security"

Session 4: Network Forensics

- Analysis of Network Logs
- Analysis of Packet Captures

Session 5: Email and Browser Forensics

- Email Forensics
  - o Various Email Based Attacks
  - o Email Header & Content Analysis
- Browser Forensics

Session 6: Using TI and Reporting

- Using Threat Intelligence in Investigations
- Sources of Threat Intelligence
- Report Writing

Examination – The participants would need to undergo an online examination after the training. On successfully clearing the examination, the participant would be awarded with the CPFA certificate

"Remember….. you are the Centre of Security"

Trainer Details

**Lionel Faleiro,
Practice Lead - Forensics
Network Intelligence**

Lionel is passionate about training and working in DFIR. He comes with an experience of almost 10 years in IT and Cybersecurity. He began as a SysAdmin then a Security Trainer and now leads the Forensic Practice at the firm. He has solved numerous cases during his tenure at Network Intelligence and is an avid gamer as well.

Registration link: https://forms.office.com/r/cwbrzsXcZm