Certified Professional Forensics Analyst (CPFA)

A 12 hours of training on forensics

Batch 1: Asia & Middle East
Date: 16-18 August 2023
Timing: 6:00 am – 10:00 am GMT
Mode of training: Online

Batch 2: Americas & Europe
Date: 21-23 August 2023
Timing: 1:00 pm – 5:00 pm GMT
Mode of training: Online

Course Fees:

USD 200 for Regular Participants

USD 150 for ISACA/ISC2 Members

NETWORK INTELLIGENCE
The Digital Security Company

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.

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

Why CPFA?

The term cybercrime no longer refers only to hackers and other external attackers. Almost all financial fraud or employee misuse cases involve 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 the start to end of digital forensics investigation, incident detection, and response.

Objectives

- What should one do when a computer-based crime is suspected?
- What tools and techniques are most likely to yield the right clues?
- What is the procedure for dealing with incident response and remediation?
- How should the investigation be carried out such that it can be presented in a court of law?
- Demonstration with the world's leading forensics tool – Encase

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 training experience with case studies to explain the digital forensics and incident response process in much detail.

Course Content

Session 1: Computer Crimes & Case Studies

- Hacking Incidents
- Financial Theft
- Identity Theft
- Corporate Espionage
- Email Misuse
- Case Studies

Session 2: Introduction to Incident Response

- Pre-incident Preparation
- Detection of Incidents
- Initial Response Phase
- Response Strategy Formulation
- Incident Management Process
- Writing An Incident Response Plan
- Incident Response Runbooks
- SIEM Use Cases – Kill Chain

Session 3: Digital Forensics

- Introduction to Digital Forensic
- Chain of Custody
- Evidence Collection & Analysis
- The 6 A's of Digital Forensics
- Network Forensics
- Live Forensics
- Windows Live Response
- Linux Live response
- Browser Forensics

" Prevent a security breach by keeping data out of reach "

Course Content

Session 4: Forensic Imaging

- Introduction to Imaging
- Importance of Imaging
- Integrity of the Evidence
- Disk Imaging using Encase / FTK
- Write Blockers
- Memory Analysis
- Tools for Acquiring RAM Dump
- Volatility Framework
- Email Forensics
- Introduction to Steganography

Session 5: Finding IOC's & Forensic Report Writing

- Gathering Indicators of Compromise (IOC's)
- Report Writing Skills
- Sample Report
- Common Mistakes in Reports

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

Trainer Details

Mufaddal Taskin

Training Specialist & Cyber Security Consultant, Network Intelligence

Mufaddal is a highly experienced professional with over 25 years in technology solutions. Currently, he holds dual roles as a Security Analyst and Training Specialist at Network Intelligence. His primary focus revolves around Security Trainings, Vulnerability Assessment, and Penetration Testing. Mufaddal possesses extensive technical abilities encompassing Networks, Web Apps, Incident Response, Cyber Threat Intelligence, SOC, and ISO standards Compliance. Moreover, he has successfully developed customized course outlines and delivered training sessions to various clients of Network Intelligence.

.

Udit Pathak,
Head of Department– Compliance and Audit,
Network Intelligence

Udit has rich experience of 10+ years in the field of information security and Audits. He has carried out PCI DSS audits, ISO27001, Vulnerability assessments, System and Server Audits, Web application security assessments, Secure code reviews, Technical security assessments, Vendor Audits, HIPAA Implementation & Audits, and SOC maturity assessments. Udit heads the Compliance & Audit Delivery channel at Network Intelligence. He has delivered excellent projects across the globe for the payment ecosystem, BFSI, the travel industry, health care, and defense services for both cloud and traditional on-prem solutions.

Registration Link: https://forms.office.com/r/9XJQrnkUqa