GIT

Creating IT Professional

CYBER SECURITY MASTER PROGRAM

Your passport to become cyber security professional

www.gitinfo.com ☎ +91 99721 77745 / +91 9535260987 training@gitinfo.com

GIT

Creating IT Professional

GIT Academy offers a comprehensive Cyber Security Master training program that provides students with the skills and knowledge necessary to succeed in the field of cybersecurity. The program covers a wide range of topics, including network security, cryptography, ethical hacking, cyber law and policy, and information assurance. Students in the program have the opportunity to gain hands-on experience through internships, research projects, and lab exercises. The program also offers networking opportunities with industry professionals and potential employers. Graduates of the Cyber Security Master training program are well-prepared for careers in cybersecurity management, network security, and information assurance, making it an excellent choice for individuals seeking to advance their careers in the cybersecurity field.

GIT
Creating IT Professional

10 CORE TRACKS

- ➢ Networking+
- ➢ Security+
- ➢ Python Scripting
- ➢ Cisco Certified Network Associate Course – CCNA
- ➢ Certified Ethical Hacking version 12 – CEHv12
- ➢ Bug Bounty Hunting
- ➢ Certified Security Operations Center Analyst
- ➢ Computer Hacking Forensic Investigator – CHFI
- ➢ Certified Penetration Testing Professional – CPENT
- ➢ Real Time Projects

www.gitinfo.com +91 99721 77745 / +91 9535260987 training@gitinfo.com

GIT
Creating IT Professional

Networking+

Network+ validates the technical skills needed to securely establish, maintain and troubleshoot the essential networks that businesses rely on. Network+ prepares candidates to support networks on any platform. Network+ is the only certification that covers the specific skills that network professionals need.

COURSE MODULE:

Duration: 40 Hours

Domain

Module 1: Network Concepts
Module 2: Network Installation and Configuration
Module 3: Network Media and Topologies
Module 4: Network Management
Module 5: Network Security

GIT
Creating IT Professional

Security+

Security+ opens the door to your cyber security career!
Security+ is a global certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career.

COURSE MODULE:

Duration: 40 Hours

Module 1: THREATS, ATTACKS, AND VULNERABILITIES
Module 2: ARCHITECTURE AND DESIGN
Module 3: IMPLEMENTATION
Module 4: PERATIONS AND INCIDENT RESPONSE
Module 5: GOVERNANCE, RISK, AND COMPLIANCE

GIT
Creating IT Professional

Python Scripting

Python Scripting allows programmers to build applications easily and rapidly. This course is an introduction to Python scripting, which focuses on the concepts of Python. It will help you to perform operations on variable types. You will learn the importance of Python in real time environment and will be able to develop applications based on the Object-Oriented Programming concept.

COURSE MODULE:

Duration: 20 Hours

Module 1: Introduction to Python Language
Module 2: Download & Install Python
Module 3: Python Language Syntax
Module 4: Python Keywords and Identifiers

Module 5: Python Comments

Module 6: Python Variables

Module 7: Python Data Types

Module 8: Python Operators

Module 9: Python Control Flow – Decision Making

Module 10: Python Control Flow – Looping

Module 11: Python Numbers

Module 12: Python Strings

GIT
Creating IT Professional

Cisco Certified Network Associate Certification Course - CCNA

CCNA Training proves you have what it takes to navigate the ever-changing landscape of IT. CCNA exam covers networking fundamentals, IP services, security fundamentals, automation, and programmability.

Designed for agility and versatility, CCNA validates that you have the skills required to manage and optimize today's most advanced networks.

COURSE MODULE

Duration: 40 Hours

Module 1: Network Fundamentals
Module 2: Network Access
Module 3: IP Connectivity
Module 4: IP services & security
Module 5: Wireless
Module 6: Automation

Certified Ethical Hacking version 12 – CEH v12

- Build Your Career with the Mist In-Demand Ethical Hacking Certification in the World, Certified Ethical Hacker
- The World’s Number 1 Ethical Hacking Certification
- A Structured Professional Course for Aspiring Cyber Professionals
- Work Anywhere With C|EH- It’s Globally Recognized
- Comprehensive Program to Master the 5 Phases of Ethical Hacking
- Hands-On Learning With CyberQ
- C|EH is divided into 20 modules and delivered through a carefully curetted training plan that typically spans 5 days. As you progress through your training, each module offers extensive hands-on lab components that allow you to practice the techniques and procedures taught in the program in real time on live machines.

COURSE MODULE:

Duration: 40 Hours

Module 1: Introduction to Ethical Hacking
Module 2: Footprinting and Reconnaissance
Module 3: Scanning Networks
Module 4: Enumeration
Module 5: Vulnerability Analysis
Module 6: System Hacking
Module 7: Malware Threats
Module 8: Sniffing
Module 9: Social Engineering
Module 10: Denial-of-Service
Module 11: Session Hijacking
Module 12: Evading IDS, Firewalls, and Honeypots
Module 13: Hacking Web Servers
Module 14: Hacking Web Applications
Module 15: SQL Injection
Module 16: Hacking Wireless Networks
Module 17: Hacking Mobile Platforms
Module 18: IoT Hacking
Module 19: Cloud Computing
Module 20: Cryptography

GIT
Creating IT Professional

Bug Bounty Hunting

This course “Practical Bug Bounty Hunting for Hackers and Pentesters, will guide you from finding targets, over developing exploits to writing comprehensive reports and ensure your success in the Bug Bounty industry.
By the end of this course, with hands-on examples and real-world tricks, you will soon be able to find your first bug.

COURSE MODULE:

Duration – 40 Hours

Module 1: About Cyber Security Industry
Module 2: Setting up Hacking Machine
Module 3: Introduction to Networking
Module 4: Web Application Fundamentals & Configurations
Module 5: Introduction to Web Application Security Testing
Module 6: Web Application Reconnaissance
Module 7: Working with Burp suite

Module 8: Exploiting Traditional Web Application Vulnerabilities
Module 9: Introduction to Session Managements
Module 10: Introduction to XSS (Cross-Site Scripting)
Module 11: Introduction to SQL injection
Module 12: Introduction to File Inclusion Vulnerability
Module 13: CSRF (Cross-Site Request Forgery Attack)
Module 14: SSRF (Server-Side Request Forgery Attack
Module 15: IDOR (Insecure Direct Object Reference)
Module 16: OS Command injection
Module 17: Response Manipulation
Module 18: Host Header Injection
Module 19: Parameter Tampering
Module 20: XXE (XML External Entity)
Module 21: RCE (Remote Code Execution)
Module 22: Introduction to Bug Bounty Platforms

GIT
Creating IT Professional

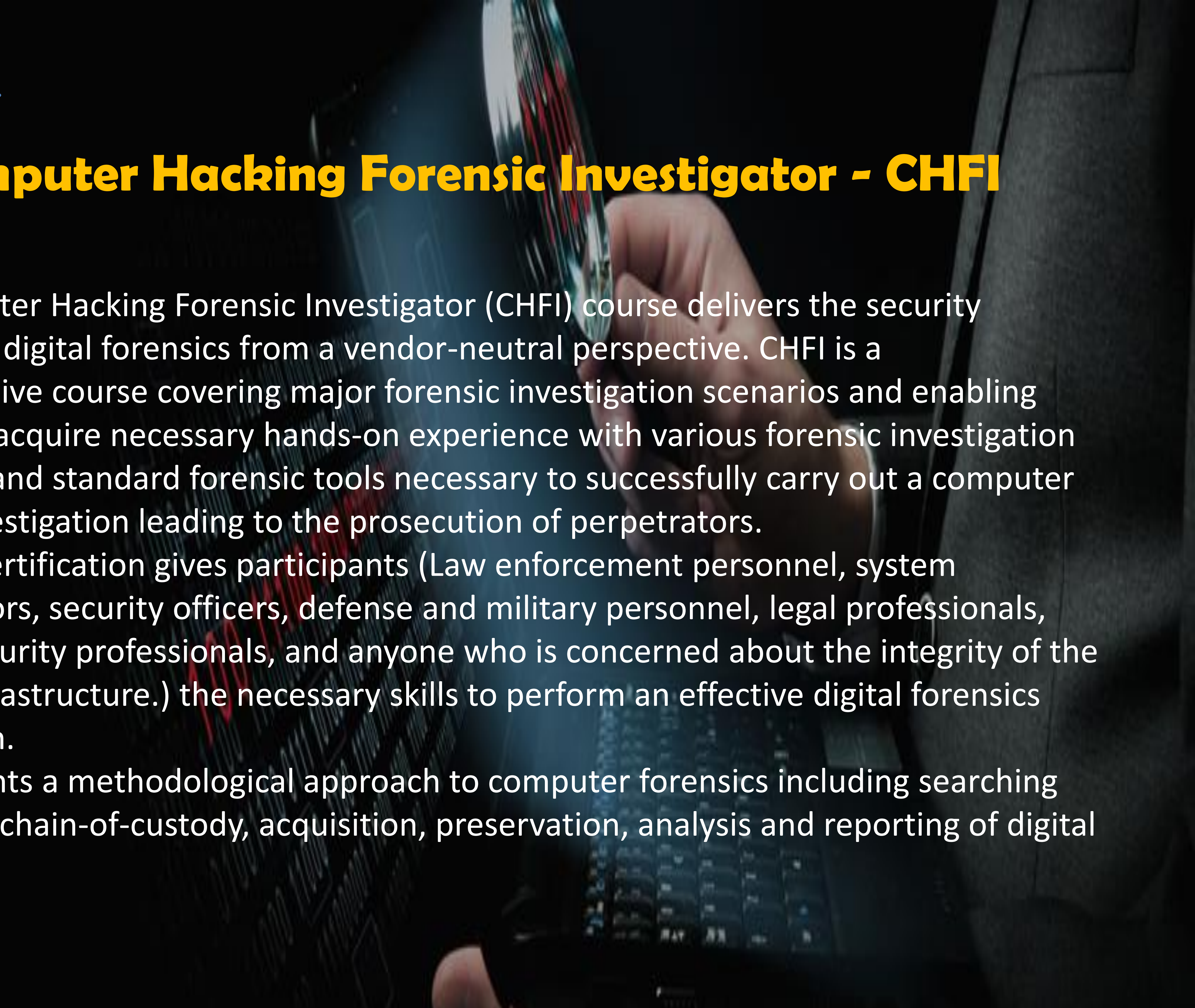
Certified Security Operations Center Analyst - CSA

The Certified SOC Analyst (CSA) program is the first step to joining a security operations center (SOC). It is engineered for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entry-level and intermediate-level operations.

COURSE MODULE:

Duration: 24 Hours

Module 1: Security Operations and Management
Module 2: Understanding Cyber Threats, IoCs, and Attack Methodology
Module 3: Incidents, Events, and Logging
Module 4: Incident Detection with Security Information and Event Management (SIEM)
Module 5: Enhanced Incident Detection with Threat Intelligence
Module 6: Incident Response



Computer Hacking Forensic Investigator - CHFI

- The Computer Hacking Forensic Investigator (CHFI) course delivers the security discipline of digital forensics from a vendor-neutral perspective. CHFI is a comprehensive course covering major forensic investigation scenarios and enabling students to acquire necessary hands-on experience with various forensic investigation techniques and standard forensic tools necessary to successfully carry out a computer forensic investigation leading to the prosecution of perpetrators.
- The CHFI certification gives participants (Law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure.) the necessary skills to perform an effective digital forensics investigation.
- CHFI presents a methodological approach to computer forensics including searching and seizing, chain-of-custody, acquisition, preservation, analysis and reporting of digital evidence.

COURSE MODULE

Duration: 40 Hours

Module 1: Computer Forensics in Today's World
Module 2: Computer Forensics Investigation Process
Module 3: Understanding Hard Disks and File Systems
Module 4: Data Acquisition and Duplication
Module 5: Defeating Anti-Forensics Techniques
Module 6: Windows Forensics
Module 7: Linux and Mac Forensics
Module 8: Network Forensics
Module 9: Investigating Web Attacks
Module 10: Dark Web Forensics
Module 11: Database Forensics
Module 12: Cloud Forensics
Module 13: Investigating EmailCrimes
Module 14: Malware Forensics
Module 15: Mobile Forensics
Module 16: IoT Forensics

Certified Penetration Testing Professional - CPENT

CPENT program is all about the pen test and will teach you to perform in an enterprise network environment that must be attacked, exploited, evaded, and defended. If you have only been working in flat networks, CPENT's live practice range will teach you to take your skills to the next level by teaching you to pen test IoT systems, OT systems, as well as how to write your own exploits, build your own tools, conduct advanced binaries exploitation, double pivot to access hidden networks, and customization of scripts and exploits to get into the innermost segments of the network.

COURSE MODULE:

Duration: 40 Hours

Module 1: Introduction to Penetration Testing
Module 2: Penetration Testing Scoping and Engagement
Module 3: Open Source Intelligence (OSINT)
Module 4: Social Engineering Penetration Testing
Module 5: Network Penetration Testing – External
Module 6: Network Penetration Testing– Internal
Module 7: Network Penetration Testing – Perimeter Devices
Module 8: Web Application Penetration Testing
Module 9: Wireless Penetration Testing
Module 10: IoT Penetration Testing
Module 11: OT/SCADA Penetration Testing
Module 12: Cloud Penetration Testing
Module 13: Binary Analysis and Exploitation
Module 14: Report Writing and Post Testing Actions

REAL TIME PROJECT

A real-time project is a practical approach to cybersecurity training that allows learners to apply their theoretical knowledge in real-world scenarios. In a cybersecurity real-time project, learners are tasked with identifying vulnerabilities in a computer system, developing security measures to mitigate those vulnerabilities, and testing those measures for effectiveness. By engaging in a real-time project, learners gain hands-on experience in various areas of cybersecurity such as network security, application security, and cloud security. Additionally, they learn critical skills like threat intelligence analysis, incident response, and risk management. A cybersecurity real-time project is a great way for learners to gain practical experience in the field and prepare themselves for real-world challenges they may face as cybersecurity professionals.

Program Benefits

- ➢ Receive 280 hours of expert-led training from experienced instructors.
- ➢ Get personalized attention and one-on-one doubt resolution sessions.
- ➢ Engage with interactive and stimulating training materials.
- ➢ Utilize industry-standard tools and software to prepare for certification exams.
- ➢ Benefit from ongoing updates and enhancements to training materials to stay up to date with the latest trends and practices.
- ➢ Join a community of fellow learners and cybersecurity professionals to network and exchange ideas.
- ➢ Receive job assistance to help launch or advance your career in the cybersecurity field.

Course Fees INR 121427/-

Discount – 30%

Training Fees (With Discount) – INR 84999/-