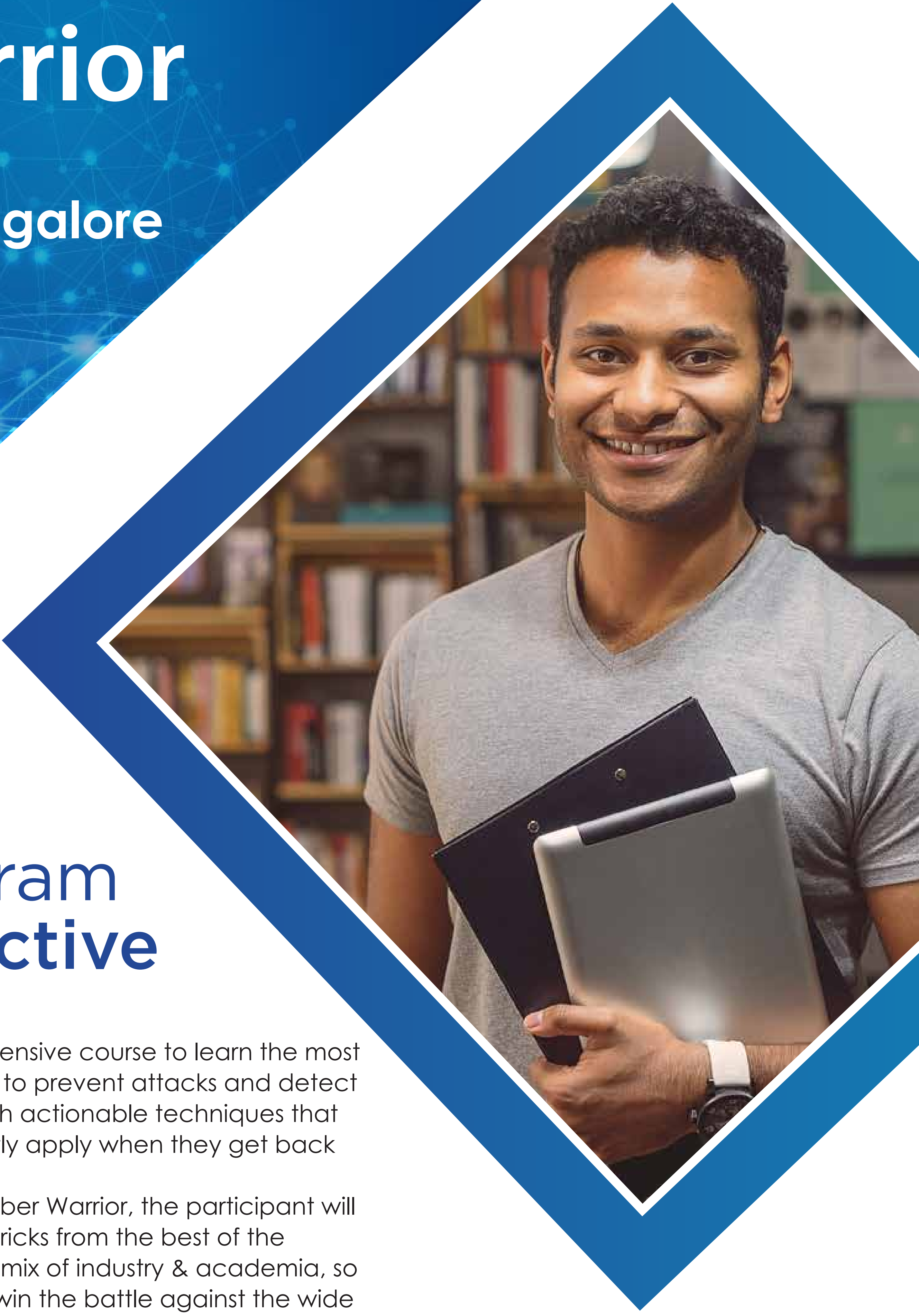
Certified Cyber Warrior

from

IIIT Bangalore



Program Objective

It is a comprehensive course to learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that one can directly apply when they get back to work.

As Certified Cyber Warrior, the participant will learn tips and tricks from the best of the experts from a mix of industry & academia, so that they can win the battle against the wide range of cyber adversaries that want to harm the enterprises' IT environment.

Predict Detect Protect FISST

TALENTEDGE
Live & Interactive Digital Learning

Program Highlights

On successful completion of the program, you will be able to

- Apply what you learnt directly to your job when you get back to work.
- Design and build a network architecture using VLANs, NAC, and 802.1x based on advanced persistent threat indicators of compromise.
- Run Windows command line tools to analyze the system looking for high-risk items.
- Run Linux command line tools (ps, ls, netstat, etc.) and basic scripting to automate the running of programs to perform continuous monitoring of various tools.
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/security of systems.
- Create an effective policy that can be enforced within an organization and design a checklist to validate security and create metrics to tie into training and awareness.
- Identify visible weaknesses of a system using various tools (mostly free or minimal subscription – without large investment) and, once vulnerabilities are discovered, cover ways to configure the system to be more secure.
- Build a network visibility map that can be used for hardening of a network - validating the attack surface and covering ways to reduce that surface by hardening and patching.
- Sniff open protocols like telnet and ftp and determine the content, passwords, and vulnerabilities using WireShark and many more relevant tools.

Other benefits to participants include

- Opportunity to earn a Certificate from IIIT Bangalore.
- Lectures imparted by eminent academicians and practicing industry experts.
- Get exposure to contemporary and sought after areas like Cyber Insurance, Blockchain, Cryptocurrencies etc.
- Gain comprehensive understanding of applicable Cyber Laws.
- 2 days On Campus "Bootcamp" style workshop module covering hands-on exposure to 30+ tools, lab sessions on Cyber Threats and Cryptography.
- Certificate Distribution Ceremony on campus at the completion of the program
- Fully Online Course with LIVE online interactive lectures that provides a "real" classroom experience in a "virtual" environment. No isolated learning experience.
- Seamless technology that can transmit lecture videos effectively at home broadband connection of 512 kbps.
- User friendly and easy to use technology interface. No expensive and time consuming software/hardware installations required at your end.
- Virtual classrooms that allow for active interactions with other fellow students and faculty.
- NFC chip-enabled certificate with security features.
- Convenient weekend schedules.
- In the event that students miss attending the LIVE lecture on the Virtual Classroom for some reason, students will be granted access to the recorded sessions for a specified number of days/times.
- TALENTEDGE's SLIQ Cloud Campus – Students on our virtual social learning platform are provided access to course presentations, projects, case studies, assignments and other reference materials as applicable for specified courses. Students can raise questions and doubts either real time during the live class or offline through the Cloud Campus.
- Learn from Anywhere – No need to travel to an institute or training center. Learning continues even if you are traveling or not available at any specific location. You may also learn from the comfort of your home.

Syllabus

Module 1: Cyber Security Foundation Module

- Introduction & Overview of Cyber Security
- Common Security threats and prevention / mitigation plans
- Cryptography – fundamentals with theory of encryption keys (LMS)
- Networking Security – fundamentals with N/w layers and various protocols (LMS)

Module 2: Introduction to IT Act and Cyber Laws

- Cyber Laws – Overview of Cyber Civil Wrong
- Cyber Laws – overview of Cyber Offences
- Case studies where brand and financial loss has been reported

Module 3: Introduction to Dark web and Deep Web

- Dark web & Deep Web
- Anatomy of Financial Cyber Crime Organization

Module 4: Network Security & Best practices for secured n/w administration

- VPN
- Wireless Security

Module 5: Vulnerabilities in various layers of Information Systems

- Overview of Multitasking and Multiprocessing
  - Assess And Mitigate Security Vulnerabilities
  - Understanding Security Capabilities of Information System
- Virtualization
- Memory Protection
- Memory & Address protection
- Protection Mechanisms

Module 6: Brief Introduction to Cyber Risk and Cyber Insurance Best Practices

- Cyber Risk & Information Risk Management
  - Risk Management Concepts
  - Component of Risk Management – example
  - Risk Management Process
  - Common Cyber Threats
  - Framework for Cyber and IS Risk
  - Management
- Cyber Insurance - an Introduction
  - What is cyber insurance
  - How to assess and bargain a good policy
  - How to implement documentation for claims
  - Best practices for 'zero' risk policies

Module 7: Introduction to Physical Security & importance to protect IT Assets

- Physical Security Introduction
- Perimeter / Boundary Security
- Building Security
- Inside Building with back end command & control System
- Overview of IoT devices Security & Concerns

Module 8: Introduction to Blockchain, Cryptocurrencies and Bitcoins

- Introduction to Blockchain concept
- Cryptocurrencies

Module 9: Cyber Security Design and Maintaining Resilience

- Cyber Security Designing And Maintaining Resilience
- Designing a Resilient Enterprise
- Maintaining Enterprise Resilience
- Perimeter Protection with Firewall
- Incident Response Plan
- Cyber Risk Management process
- Inventory Authorized and Unauthorized devices and Software

Module 10: Recommended Best practices for Cyber Security

- Cyber Hygiene
- Data Security
- Wireless networking
- Invoke the Incident Response Plan
- Recover
- RTO – RPO
- Preparedness Plan Audit
- Test your incident response plan
- Vendor Incident response

Module 11: 20 Critical Security Components – Part 1

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Controlled Use of Administrative Privileges
- Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 7: Email and Web Browser Protections
- Critical Control 8: Malware Defenses
- Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services

Module 12: 20 Critical Security Components – Part 2

- Critical Control 10: Data Recovery Capability
- Critical Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Critical Control 12: Boundary Defense
- Critical Control 13: Data Protection
- Critical Control 14: Controlled Access Based On Need to Know
- Critical Control 15: Wireless Device Control
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 18: Application Software Security
- Critical Control 19: Incident Response and Management
- Critical Control 20: Penetration Tests and Red Team Exercises

2 Day On Campus Boot Camp at IIIT B

- Lab Session – General Threats
- Lab Session – Cryptography
- Boot Camp 1
- Boot Camp 2

About IIIT Bangalore

The International Institute of Information Technology, a Deemed University, popularly known as IIIT-B, was established in 1999 with a vision to contribute to the IT world by focusing on education and research, entrepreneurship and innovation. The Institute is a registered not-for-profit society funded jointly by the Government of Karnataka and the IT industry.

Since its inception, IIIT-B, with its unique model of education, research, and industry interaction, has grown in stature to become an institution of considerable repute in academic as well as corporate circles. The Institute works in partnership with the corporate sector while retaining the freedom of an academic institution. It is inspired by other renowned institutions, and also strives to emulate an academic culture that is on par with the best international institutions.

The incubation Centre at IIITB has done well by incubating a number of successful startups. It has incubated 50 plus startups, over 80 new products/services were brought to market, over 300 jobs have been created and over 10 startups managed to raise funds.

About FISST

Forensics Intelligence Surveillance and Security Technologies (FISST) as the name suggest works on the entire stack of Security Technologies starting from Sensors / Capturing devices to Surveillance to Intelligence and Forensics, both Physical and Cyber technologies space.

FISST has tie-ups with leading academic institutes in India like IIT-Madras, IIIT-Bangalore as well as international institutes such as Virginia Technology, USA for offering Cyber Security Education to various target groups. We have already trained staff from leading banks such as Canara Bank, Vijaya Bank, IDFC Bank, AXIS Bank as well as e-Gov + Treasury department of Govt. of Karnataka, L&T Shipbuilding, Dredging Corporation, Indus software etc. with tools & techniques to ‘Assess, Predict, Detect and Protect’ the IT Assets of these organisations.

FISST has started building some Cyber Security related products relevant to Indian market (as most of the tools are imported and it is expensive). These will hit the market by end of 2019.

There is no entity across World with full suite with whole stack of FISST and we aim to be in Global Market in next 3 years as part of ‘Make in India’ for Security and Surveillance.

MR. MOHAN RAM CHANDRASEKAR

Visiting Faculty @ IIIT-B &
Program Director – CCSER

Mohan has nearly 32 years of professional experience after an M.Tech from IIT-Roorkee, as IT leader specializing in Cyber Security and related physical surveillance for critical infrastructure including refinery, nuclear power plants and mission critical IT infrastructure etc. Mohan is currently pioneering Cyber Education space in India to create awareness and fill the gap in skills to tackle potential damages due to cybercrimes in partnership with leading academic institutions across India.

Lead Academic Faculty Members:

Ashish Choudhury

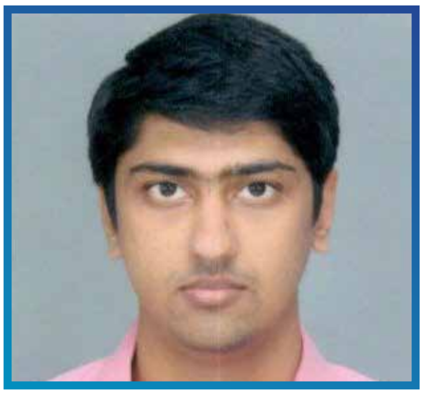
Assistant Professor & Infosys Foundation
Career Development Chair Professor

Dr. Ashish Choudhury received his MS (by Research) and Ph.D degree from Indian Institute of Technology, Madras in 2006 and 2010 respectively. After his Ph.D he worked as a visiting scientist at Indian Statistical Institute Kolkata for a year and then as a research assistant for two years at University of Bristol. His research interest include theoretical cryptography, with specialization in cryptographic protocols.

Tricha Anjali

Associate Professor
& Associate Dean
(Continuing
Professional
Education)

Prof. Anjali received her Integrated M.Tech. (EE) from Indian Institute of Technology, Bombay in 1998 and Ph.D. from Georgia Institute of Technology in Atlanta in 2004. Since 2004 she has been with the Department of Electrical and Computer Engineering at Illinois Institute of Technology, Chicago. Her broad research interests include computer networks and wireless networks. More specifically, design and analysis of multipath routing schemes, heterogeneous radio access network selection and game theoretic approaches.



Dr. Harish Ramani

PhD in Underwater
Wireless
Communication,
Australia

Harish Ramani is the Founder Director & Chief Technology Officer of Internettechies, a Chennai based Start-up. He has about 7 years of experience in the field of Networking, Communication and Security. His research was in the field of Underwater Wireless Communication. He has delivered 100+ workshops and Seminars in colleges, Universities and Corporates. He has served with Chennai Cybercrime Police department and worked many critical cases like money theft, social media postings and finding critical information. Other prominent names he has been associated with are Ford India, Catholic Syrian Bank, NHIF Kenya, BharatRE, Kotak Bank, Bank of Baroda and Axis Bank in various capacities.

Eligibility

- For Indian Participants - Graduates or Diploma Holders (10+2+3) from a recognized university (UGC/AICTE/DEC/AIU/State Government) in any discipline.

- For International Participants - Graduation or equivalent degree from any recognized University or Institution in their respective country.

Pre Requisites

- Basic understanding of technology, networks and security, while not mandatory, will be an added advantage.

Who Should **Attend**

Working professionals and fresh students aspiring to have a career in Cyber Security can enroll for this program. Anyone who works in security, is interested in security, or has to understand security should take this course, including:

- Security professionals who want to fill the gaps in their understanding of technical information security.
- Managers who want to understand information security beyond simple terminology and concepts.
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective.
- IT engineers and supervisors who need to know how to build a defensible network against attacks.
- Administrators responsible for building and maintaining systems that are being targeted by attackers.
- Forensic analysts, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs.
- Anyone new to information security with some background in information systems and networking.

Pedagogy

The primary method of instruction will be through LIVE lectures that will be delivered online via internet to participant desktops/laptops or classrooms. The lectures will be delivered by eminent academicians and practicing industry experts. The program will be primarily taught though a combination of lectures, discussions, exercises and labs. All enrolled students will be provided access to our SLIQ Cloud Campus through which students may access other learning aids, reference materials, assessments and assignments as appropriate. Throughout the duration of the course, students will have the flexibility to reach out to the Professors, real time during the class or offline via the SLIQ Cloud Campus to raise questions and clear their doubts.

Assessment

There are periodic evaluation components built in as a part of the program. These maybe in the form of a quiz, assignment or other objective/subjective assessments as relevant and applicable to the program. A minimum of 70% attendance to the LIVE lectures and participation in the 2 Day on-campus boot-camp, is a prerequisite for the successful completion of this program. Participants who satisfy the attendance criteria and successfully clear the evaluation components will be awarded a certificate of completion.

Schedule and **Fees**

- Course Start Date: 29th April 2018
- Class timings: Twice a week on Saturdays and Sundays from 10.00 a.m. to 12.00 p.m.
- Course Duration: 4 months
- Indian Participants: INR 98,000 + GST
- International Participants: USD 2000

How to **Apply**

For admissions, students can register at : **www.talentedge.in**

For more **details**

Students can write in to - **enquiry.dtd@talentedge.in** or call at **+91-83760 00600**

Talentedge, CBIP Building, 5th floor, Plot No - 21, SECTOR-32, Gurgaon - 122003

TALENTEDGE
Live & Interactive Digital Learning

iiit-b

Predict
Detect
Protect
FISST