



International
Institute of Information
Technology Bangalore

simplilearn

AI-Powered Advanced Executive Program in Cybersecurity

In collaboration with



Elite Training Partner

EC-Council



AI-Driven Career
Launchpad



100+ Guided
Projects & 30+ Tools



CEH v13 AI Voucher
Exam Included*

Table of Content

AI x Cybersecurity: The Future Is Here	3
The All-in-One Cybersecurity Program for the AI Era	4
AI x Cybersecurity: Key Features of the Program	5
Learning Path	6
Skills Covered	10
Learning Outcomes	11
Case Studies	12
Integrated Labs & Tools	13
Capstone Project	14
Certificates	15
Career Outlook in the Cybersecurity Industry	16
Advisory Board	17
Eligibility Criteria	19
Application Process	19
Talk to an Admissions Counselor	19

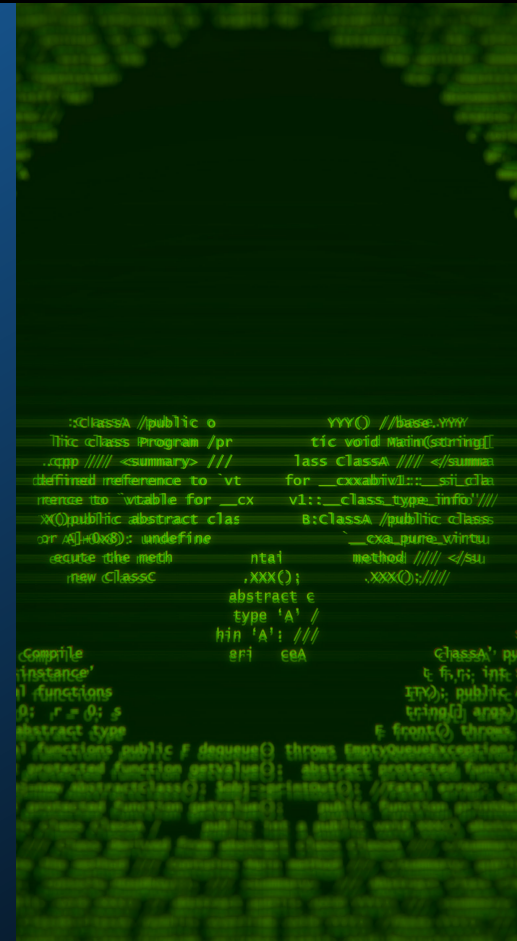
AIx Cybersecurity: The Future Is Here

Cyber threats are evolving, and AI is reshaping the battlefield.

The Shift – Cyber Threats Are Evolving

Cyber threats today aren't just faster; they're smarter, more adaptive, and increasingly AI-driven. From automated exploits to intelligent defence, the battlefield is evolving. As adversaries weaponize AI to scale attacks, the need for AI-enabled security professionals has never been greater.

- ✔ **78%** of security teams report AI-powered threats. (Darktrace)
- ✔ AI speeds up detection and response by **28%**, minimizing damage and saving \$1.76M per breach. (IBM)
- ✔ **53%** of companies have adopted AI in cybersecurity. (Ponemon Institute)



The Urgency – India's Cybersecurity Landscape

India's cybersecurity market is growing rapidly, driven by digital expansion and rising threats:

- ✔ Market projected to grow from **\$4.7 billion in 2024 to \$10.9 billion by 2029**. (Wright Research, 2024)
- ✔ Only **24%** of organizations are fully equipped to handle cyber threats, while 49% struggle to hire skilled professionals. (Expert Market Research, 2024)

The Impact – AI Is Redefining Security

- ✔ Speeds up threat detection and response by **28%**, reducing potential damage. (IBM)
- ✔ Helps organizations save **\$1.76 million** per breach. (IBM)
- ✔ **53%** of companies have already integrated AI into security operations. (Ponemon Institute)
- ✔ Attackers leverage AI to automate and accelerate breaches, creating new challenges for security teams. (Darktrace)



The All-in-One Cybersecurity Program for the AI Era

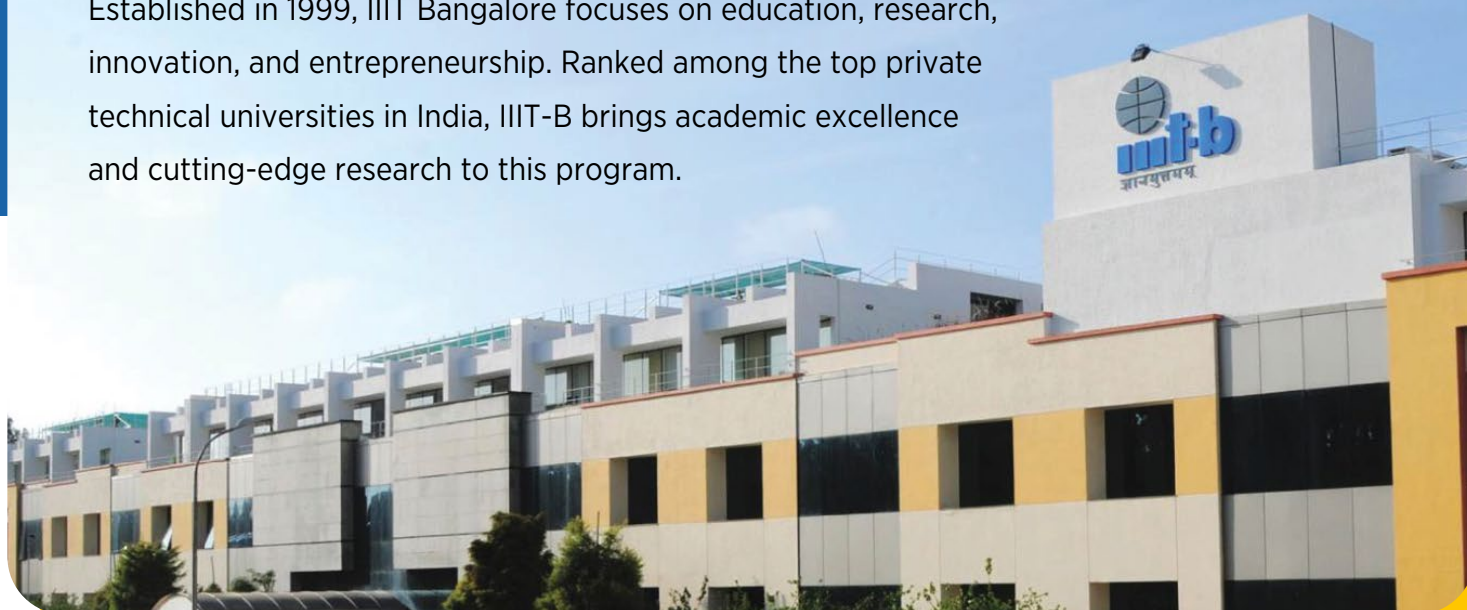
In today's rapidly evolving cyber landscape, threats are smarter, faster, and more complex than ever. To stay ahead, you need more than knowledge; you need hands-on skills, applied AI expertise, and real-world experience that employers trust.

This program takes you on that journey, combining deep cybersecurity foundations with AI-driven capabilities to detect threats, cut through noise, and respond confidently across modern hybrid environments.



Curriculum Backed by IIIT Bangalore

Established in 1999, IIIT Bangalore focuses on education, research, innovation, and entrepreneurship. Ranked among the top private technical universities in India, IIIT-B brings academic excellence and cutting-edge research to this program.



Outcome-Driven Skills



Cybersecurity Mastery

Network Security, Ethical Hacking, VAPT, Threat Hunting, and Incident Response.



AI in Cybersecurity

Exploitation & Privilege Escalation, Threat Detection, Behavioral Analytics, LLMs in Defense, and protection against Adversarial AI.

AIxCybersecurity

Key Features of the Program



Master Best-in-Class Curriculum

210+ hours of guided training by industry experts in cybersecurity and AI

- ✓ **Cybersecurity:** Foundations (OS, Networking, Cloud), Defensive (SIEM, Firewalls, IAM, Malware Analysis), Offensive (Recon, Exploitation, Post-Exploitation using Nmap, Metasploit, Burp Suite)
- ✓ **AI in Cybersecurity:** Foundational AI (GenAI, LLMs, Adversarial AI), Defensive AI (Automation & Anomaly Detection), and Offensive AI (Recon & Vulnerability Discovery)
- ✓ **Hands-On Labs:** 100+ projects, 30+ Case Studies, 30+ tools including Wireshark, Metasploit, Splunk



Aligned with Industry Trends

- ✓ EC-Council CEH v13 AI training (official kit & labs) included as part of training *
- ✓ Masterclass sessions by IIIT Bangalore faculty and former NPCI cybersecurity leader



Validate Skills & Build Portfolio

- ✓ Earn IIIT Bangalore certificate of completion (e-certificate + physical) with detailed transcript
- ✓ Showcase verified cloud and security credentials via Microsoft Learn badges
- ✓ Strengthen resume with 3 capstone projects and multiple mini-projects across offensive, defensive, and AI domains



Accelerate Career with AI-Powered Support

- ✓ AI-powered mock interviews with instant feedback
- ✓ Resume and LinkedIn guidance
- ✓ 1:1 mentoring from industry experts
- ✓ Access to curated job opportunities aligned with your skills

Learning Path

Core Courses



Electives

- Module 1 - IIITB Cybersecurity Masterclass
- Module 2 - Masterclass by Former NPCI Expert
- Module 3 - AI Literacy
- Module 4 - C|EH v13 AI - Certified Ethical Hacker
- Module 5 - Microsoft AI-Driven Cloud Security Mastery
- Module 6 - EC-Council Expert Session

Core Courses



Module 1

Preparing for your AI-Powered Cybersecurity Executive Journey

- Get an overview of the program, learning journey, and how AI is reshaping cybersecurity roles
- Understand career outcomes and the structure of your learning path



Module 2

Operating Systems & Scripting for Cybersecurity

- Build core OS security skills, covering memory, processes, and user access controls
- Learn Bash and PowerShell scripting to automate tasks and strengthen system-level defense



Module 3

Enterprise Infrastructure Security

- Dive into SOC workflows, log management, threat correlation, and alert triage
- Implement IAM policies and monitor systems using real-time SIEM platforms



Module 4

Network Security & Cryptography Essentials

- Master networking protocols and wireless security.
- Use Wireshark and cryptographic tools to secure and analyze network communications



Module 5

Application and Web Application Security

- Understand secure SDLC, OWASP Top 10, and threat modeling techniques
- Apply DevSecOps and manage vulnerabilities in secure application development



Module 6

AI Foundations for Cybersecurity Professionals

- Explore ML, NLP, deep learning, and GenAI applications in security
- Learn AI ethics, model training, and how AI supports threat detection and response



Module 7

AI-Powered Blue Team Strategies: Detection, Response & Automation

- Automate detection and response using AI and behavioral analytics
- Use threat intelligence and LLMs to enhance enterprise security posture



Module 8

Ransomware and Malware Analysis

- Track malware from payload to lateral movement and system compromise
- Conduct sandboxing, reverse engineering, and forensics for mitigation



Module 9

Ethical Hacking and VAPT

- Master red team tactics, including scanning, recon, and enumeration
- Perform recon, simulate exploits, and prioritize risks and Analyze attacker workflows to uncover and mitigate system vulnerabilities



Module 10

AI-Enhanced Red Team Tactics: Exploitation to Post-Exploitation

- Automate recon, exploitation, and persistence using AI and LLMs
- Enhance red team operations with adversarial techniques and attack simulation



Module 11

Advanced AI in Cybersecurity: LLMs, Adversarial Models & Risk Defense

- Use LLMs for SOC automation, phishing detection, and threat triage
- Defend against adversarial AI attacks across NLP and system domains



Module 12

Portfolio Project: Real-World Scenarios in Cyber, Red/Blue Teams & AI

- Solve a real-world cybersecurity scenario using red/blue team and AI skills
- Build a comprehensive portfolio project for recruiters and job readiness

Electives



IIIT Bangalore Cyber Security Master Class

- Attend online interactive Masterclasses conducted by the faculty from IIIT Bangalore
- Get insights about advancements in Cyber Security and understand the essential skills needed to become an expert in this rapidly growing domain



Masterclass by Former NPCI Expert

- Attend online interactive masterclasses conducted by former NPCI expert
- Learn about the practical application of acquired skills in Cybersecurity



CEH v13 AI Certification

- Master red teaming and AI-powered attack simulation with official labs
- Includes toolkits and exam voucher for CEH v13



Microsoft AI-Driven Cloud Security Mastery

- Self-study Azure core services covering computing, networking, and storage with emphasis on secure, scalable cloud architecture
- Explore Microsoft Security, Compliance & Identity (SC-900), AI fundamentals (AI-900), and advanced Azure security (AZ-500) through guided materials for comprehensive cloud protection
- Build career-ready skills independently to implement AI-driven security, threat detection, and identity management in cloud environments



EC-Council Expert Session

- Gain insights from a global cybersecurity authority on real-world threats and evolving industry practices.
- Stay ahead of the curve with an exclusive session led by an EC-Council expert on the latest cybersecurity trends, threat intelligence, and industry best practices.

Skills Covered

1 Cybersecurity Foundations

- Operating Systems (Windows & Linux)
- Virtual Memory, File Systems & Permissions
- Networking Fundamentals (TCP/IP, DNS, ICMP, ARP)
- WLAN Security, AAA, and Cryptography (PKI, TLS)

2 Security Operations & Defensive Practices

- SIEM, SOAR, and Log Analysis
- Threat Detection & Incident Response
- Malware, Ransomware & Forensics
- Blue Team Operations & Mitigation Tactics

3 Offensive Security & Ethical Hacking

- Reconnaissance & Enumeration
- Vulnerability Assessment & Penetration Testing (VAPT)
- Threat Modeling, Exploitation & Post-Exploitation
- Red Teaming Techniques (CEH-aligned)

4 AI in Cybersecurity

- AI & ML Fundamentals (Model Lifecycle, Ethics, Training)
- AI-Driven Threat Detection, Anomaly & Behavioral Analysis
- Automating Blue Team Operations (SIEM, SOAR)
- AI-Augmented Red Teaming (Recon, Exploit Gen, CEH AI)
- Adversarial AI & Attack Simulation

Learning Outcomes

Upon successful completion of the program, you will be able to:

- Apply core cybersecurity principles across operating systems, networking, and cryptographic protocols
- Conduct ethical hacking and vulnerability assessments aligned with CEH v13 standards
- Develop secure applications and systems using best practices in coding, risk mitigation, and threat modeling
- Detect, analyze, and respond to incidents using SIEM, log analysis, malware forensics, and threat intelligence
- Leverage AI to automate threat detection, enhance analytics, and support both defensive (Blue Team) and offensive (Red Team) operations
- Deliver a job-ready capstone project demonstrating integrated cybersecurity and AI expertise



Case Studies



*

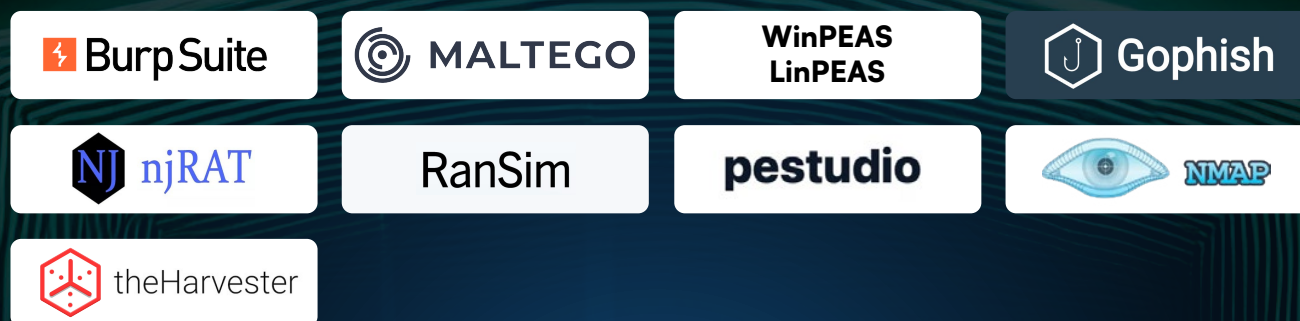
Note: All product and company names are trademarks or registered trademarks of their respective holders. Their use does not imply any affiliation with or endorsement by them.



Integrated Labs & Tools

Offensive Security Toolkit

Unleash ethical hacking and red team capabilities with precision-focused tools



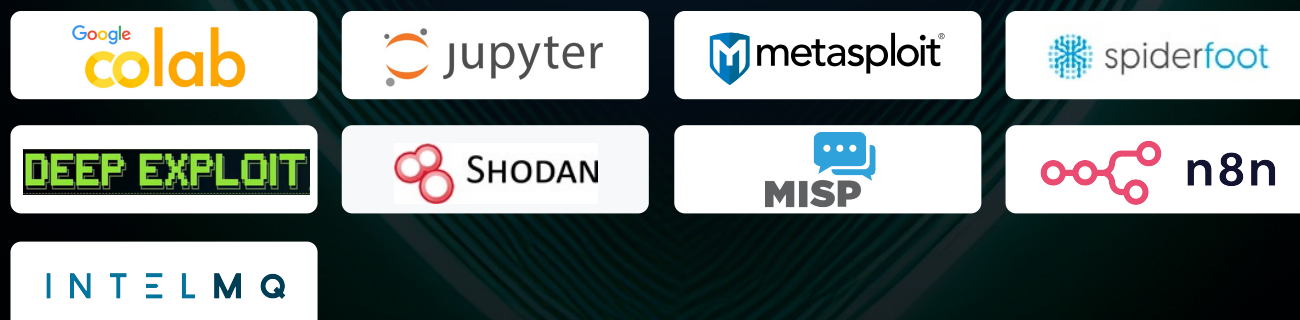
Enterprise Defense & Blue Team Stack

Build strong defensive perimeters and threat detection systems at scale



AI-Powered Cyber Intelligence Suite

Harness the power of GenAI, automation, and analytics for next-gen cybersecurity



Capstone Projects



Designing a Secure File Access and Audit System for Finance Teams

Build a secure file storage solution with access controls, command tracking, and automated violation reporting for Globex Financials project teams.



Simulating Exploitation and Remediation in a Vulnerable Network

Use tools like Nmap and Metasploit to exploit system vulnerabilities and apply remediation strategies to strengthen defenses.



Deploying and Securing Active Directory in a Windows Server Environment

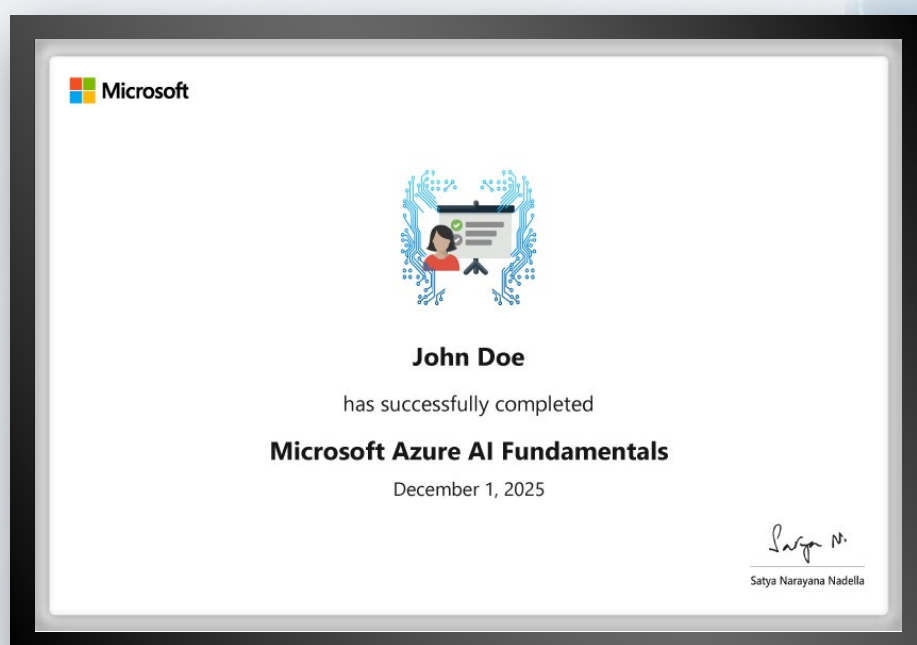
Configure domain controllers, user and group policies, and organizational units to manage access and enforce enterprise security.



Certificates



Partnership With Microsoft:



EC- Council Certification:



Career Outlook in the Cybersecurity Industry



● Senior/Expert Level (7+ years experience)

Roles: Red Team Specialist, Blue Team Specialist (Senior), Adversarial AI Specialist, Threat Intelligence Analyst (Senior)



Salary Range: ₹15–₹34 LPA

● Mid-Level (4-6 years experience)

Roles: Application Security Engineer, Cloud Security Engineer, Threat Intelligence Analyst, AI-Driven Security Operations Specialist



Salary Range: ₹12–₹25 LPA

● Entry Level (1-3 years experience)

Roles: Cybersecurity Analyst, SOC Analyst, Malware Analyst, Blue Team Specialist



Salary Range: ₹7–₹12 LPA

Advisory Board



V SRIDHAR

**Faculty In-Charge, Continuing Professional Education,
Institutional Finance**

Education : Ph.D. (University of Iowa)

Dr. V. Sridhar is Professor at the Centre for IT and Public Policy at the International Institute of Information Technology Bangalore, India. He is the author of two books published by the Oxford University Press: The Telecom Revolution in India: Technology, Regulation and Policy (2012), and The Dynamics of Spectrum Management: Legacy, Technology, and Economics (2014).

He is currently:

- ✓ Member, Advisory Committee,
Facebook India Tech Scholars Programme,
Facebook India, July 2021-Current.
- ✓ Member, Technical and Financial
Advisory Committee, E-Procurement,
Centre for E-Governance, Government
of Karnataka. Apr 2019-Current.
- ✓ Member, IT and ITeS Sectional Committee,
Services Sector Department 10, Bureau of
Indian Standards, June 2020 – Current.
- ✓ Member, Think Tank on Digital Markets,
Competition Commission of India.
Sep 2018 – Current.



SRINIVAS VIVEK

Assistant Professor

Education : Ph.D. (University of Luxembourg)

Previously, he was a (post-doctoral) Research Associate in the Cryptography group of the Department of Computer Science at the University of Bristol between Jun'15-Dec'17. Prof. Nigel Smart was his supervisor.

He obtained his Ph.D. from the University of Luxembourg, Luxembourg, in 2015.

He was affiliated to the Laboratory of Algorithmics, Cryptology and Security (LACS) in the Computer Science and Communications Research Unit. His doctoral thesis was in Cryptography and was supervised by Prof. Jean-Sébastien Coron and Prof. David Galindo.



CHANDRASHEKAR RAMANATHAN

**Professor & Dean (Academics)
& Faculty-in-charge Computing**

Education : Ph.D. (Mississippi State University)

Professor Chandrashekar Ramanathan is a faculty member at IIITB since 2007.

Professor Chandrashekar received his Ph.D degree from Mississippi State University. His thesis was in the area of object-oriented databases. He has extensive application software development experience spanning over 10 years in large multinational organizations. His current focus is in the area of information convergence and software engineering. Technology for education, Application architectures, enterprise architecture and content management are his other areas of interest.



ANTONY PRAKASH

Ex Chief Data Privacy Officer (NPCI)

With a career spanning nearly 3 decades, Mr. Antony has rich and insightful experience leading technology and security at top banking and payment organizations like SBI and NPCI, respectively. He has led information security, cybersecurity, privacy standards, and people capacity at large organizations in the Indian ecosystem. His role was pivotal in building a robust security infrastructure to manage multi-billion transactions a month for UPI at NPCI. He is also an Independent director and advisory board member for multiple organizations.



Eligibility Criteria

For admission to this **AI-Powered Advanced Executive Program in Cybersecurity**, candidates:

- ✔ Should have a bachelor's degree in any discipline with an average of 50% or higher marks
- ✔ With a non-programming background can also apply
- ✔ Should have a minimum of 4 years of work experience (preferred but not mandatory)

Application Process

The application process consists of three simple steps.



Submit an Application

Complete the application, including a brief statement of purpose explaining your interest and qualifications for the program.



Application Review

A panel of admissions counselors will review your application and statement of purpose to determine whether you qualify for acceptance.



Admission

Qualified candidates will be offered admission. You can accept this offer by paying the program fee.

Talk to an Admissions Counselor

We have a team of dedicated admissions counselors who can help you with the application process and related matters.

Our team is available to:

- ✔ Answer your questions about the application process
- ✔ Discuss your financing options
- ✔ Provide insight into the curriculum, program outcomes, and more

[Inquire Now](#)



USA

Simplilearn Americas, Inc.
5851 Legacy Circle,
6th Floor, Plano, TX 75024,
United States
Phone No: +1-844-532-7688

INDIA

Simplilearn Solutions Pvt Ltd.
53/1 C, Manoj Arcade, 24th Main Rd,
Sector 2, HSR Layout,
Bengaluru - 560102,
Karnataka, India
Phone No: 1800-212-7688

For more information, please visit:
www.simplilearn.com