simplilearn

Advanced Executive Program in Cybersecurity

In collaboration with:

iit b ज्ञानमुत्तमम्

IBM

Table of Contents:

About the Program	03
Key Features of the Program	04
About IIIT-B	05
About IBM	05
About Simplilearn	05
Integrated Labs & Tools	06
Slack Channel	07
Eligibility Criteria	08
Application Process	08
Talk to an Admissions Counselor	09
Cybersecurity Industry Trends	10
Who Should Enroll in this Program?	10
Learning Path Visualization	11
Core Topics	12
Electives	20
Capstone Projects	21
Learning Outcomes	22
Advisory Board	23
Certificate	25
Corporate Training	26
Features of Corporate Training	26

About the Program

The digital landscape has grown by leaps and bounds. Cybersecurity skills are now among the most sought-after and highly compensated as the business world has shifted towards a digital operational framework, and business data and organizational assets face an enhanced risk of cyber violations and cyberattacks. The Advanced Executive Program in Cybersecurity, a collaboration between Simplilearn, IIIT Bangalore, and IBM, is designed to empower you with the practical skills needed to enhance your organization's cybersecurity strategy. The curriculum covers various topics, from cryptography to malware analysis. It is structured to ensure you understand the theory and gain hands-on experience through practical projects and labs.

This program features the perfect mix of theory, case studies, and extensive hands-on practical experience through integrated labs. It provides a comprehensive education, leveraging IIIT Bangalore's academic excellence and Simplilearn's unique blend of self-paced online videos, live virtual classes, hands-on projects, and integrated labs.

Key Features of the Program

- Program completion certificate from IIIT Bangalore (Digital & Physical)
- Program transcript from IIIT Bangalore
- Attend masterclasses delivered by IIIT Bangalore professors
- Practice labs and projects with integrated labs
- Access to the IBM Learning Portal
- Engage in capstone projects in 3 domains
- Industry-recognized IBM certifications for IBM courses
- Exclusive hackathons conducted by IBM
- Empower your cybersecurity learning with generative AI
- Experiential learning via multiple real-life innovation projects and capstones
- Masterclass from Former-NPCI Expert
- Earn an industry-recognized Simplilearn certificate after completing each module
- Participate in live virtual classes led by industry experts, hands-on projects, and integrated labs
- Access Simplilearn's JobAssist Service to get noticed by top hiring companies

About IIIT - Bangalore

The International Institute of Information Technology Bangalore, popularly known as IIIT Bangalore was established in 1999 with a vision to contribute to the IT world by focusing on education and research, entrepreneurship, and innovation.

IIIT Bangalore has been ranked 1st among the private technical universities in India as per India Today, August 2021 edition. It has been ranked 8th overall among engineering universities in the August 2021 edition and was ranked 10th in the same category as per India Today, August 2020 edition.

About IBM

IBM Learning encompasses various programs and platforms to empower individuals with the skills and knowledge needed to succeed in the digital age. These initiatives include online courses, certifications, workshops, and learning paths covering cloud computing, artificial intelligence, cybersecurity, data science, and more.

About Simplilearn

Simplilearn is the world's #1 online Bootcamp provider, enabling learners around the globe with rigorous and highly specialized training offered in partnership with world-renowned universities and leading corporations. We focus on emerging technologies and skills transforming the global economy, such as cyber security, cloud computing, programming, and more. Our hands-on and immersive training includes live virtual classes, integrated labs and projects, 24x7 support, and a collaborative learning environment. Over two million professionals and 2000 corporate training organizations across 150 countries have harnessed our award-winning programs to achieve their career and business goals.

Integrated Labs & Tools

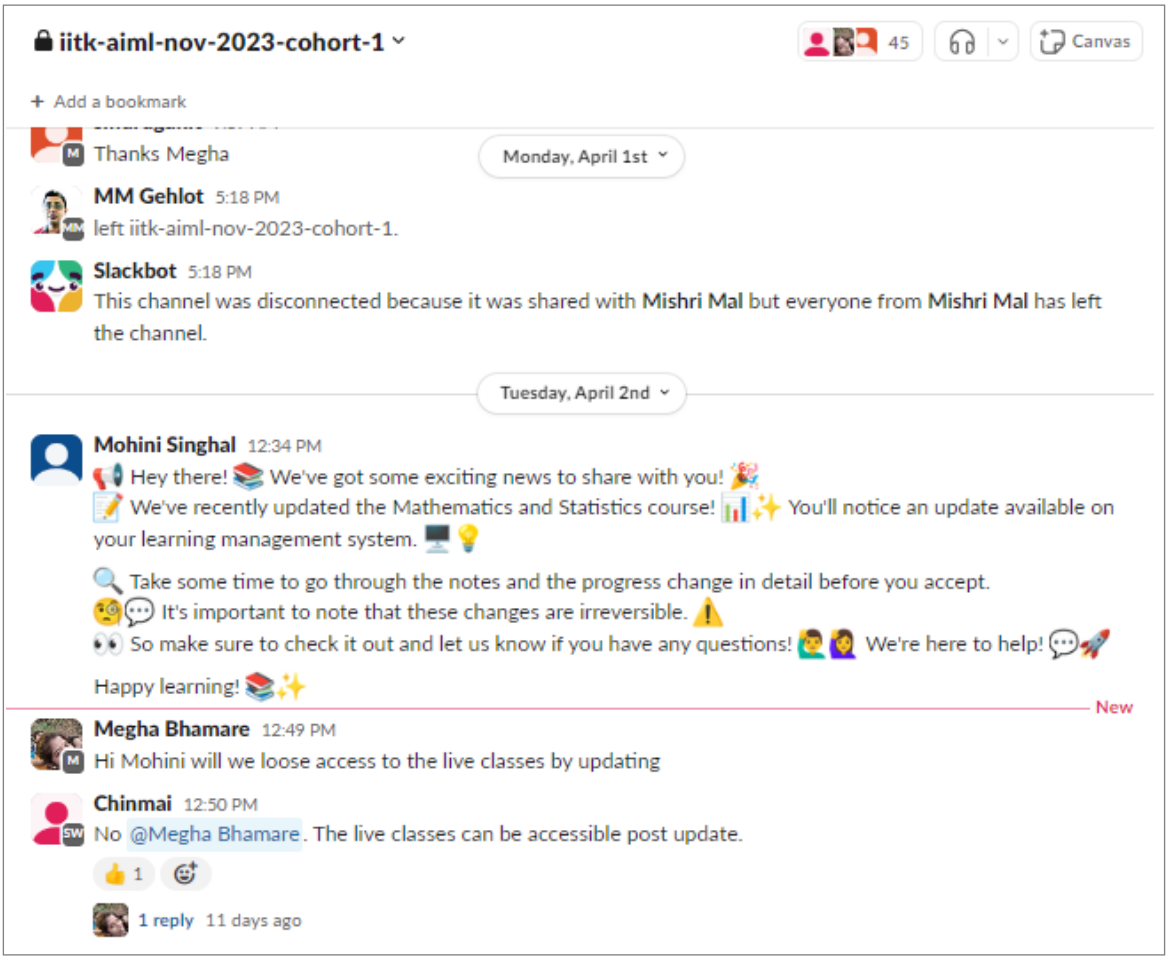
Four Virtual Machines will be provided in the laboratories (VM):

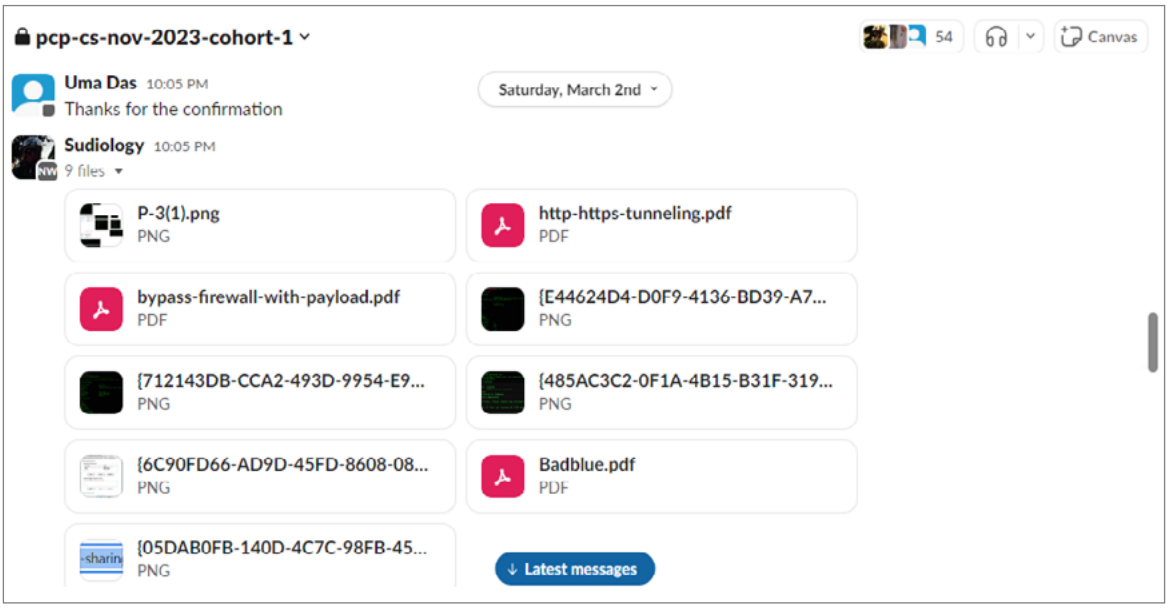
The malware listed below is malware that students wouldn't want to install on a computer but can use in our lab's virtual machine (VM). Students can simply access it without harming their PCs.

- OpenJDK
- NMap
- RanSim
- Virustotal
- Threat Dragon
- Shodan
- Nessus
- Nikto
- Crunch
- Zenmap
- Traceroute
- Exeinfo PE
- MTR
- Burpsuite
- Cuckoo
- Metasploit
- OpenVAS
- New Relic

Slack Channel

Active Engagement and Peer-to-Peer communication during and after live sessions





Eligibility Criteria

Those wishing to enroll in the program must apply for admission.

For admission to this program, 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
- Must have a minimum of 1 year of work experience

Application Process

The application process consists of three simple steps:

Step 1: Submit an Application

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

Step 2: Application Review

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

Step 3: 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

Contact Us | 1-800-212-7688

Cybersecurity Industry Trends

As per Fortune Business, The global cyber security market size is projected to grow from $172.32 billion in 2023 to $424.97 billion in 2030.

13.8% CAGR

Projected market growth between 2023-2030

Fortune Business

₹11-12 L

The average annual salary of a cybersecurity professional in India.

Glassdoor

$345 billion

Forecasted Cyber Security market size by 2026

Market.us

Who Should Enroll in this Program?

This program has been designed to meet the upskilling requirements of lower- and mid-level management professionals working in BFSI, cybersecurity, and fintech fields who have prior technical knowledge of the basics of cybersecurity. The course is ideal for people looking to work in job roles/positions such as, but not limited to:

- Security infrastructure specialists
- Network security consultants
- Security analysts
- Application security analysts
- Blue team members
- Cloud security architects
- Cybersecurity software developers
- Malware analysts
- Threat hunters

Note: *Our pre-requisite courses, which would be assigned to the learners before the start of the program, would cover the basics of cybersecurity.*

Learning Path Visualization

Core Topics

Pre-Requisites:

- Introduction to Cybersecurity
- Linux Fundamentals
- Network Fundamentals
- Cryptography

Electives:

- IIIT Bangalore Cyber Security Master Class
- Masterclass from Former NPCI Expert
- Security Governance and Framework
- IBM: Network Security & Database Vulnerabilities
- IBM: Penetration Testing, Incident Response and Forensics
- Gen AI with Cyber Security

Core Topics:

Module 1 - Induction for Advanced Executive Program in Cybersecurity

This introductory course provides an overview of the program structure, curriculum, learning outcomes, and more. You'll clearly understand what lies ahead and how this program can help you achieve your professional goals

Upon completion of this module, you will:

- Get acquainted with your peers
- Gain a complete understanding of the program

Module 2 - Enterprise Infrastructure Security

The Enterprise Infrastructure Security course will enable learners to gain knowledge and skills in a series of advanced and current concepts in cybersecurity, and related to enterprise and infrastructure security. After the completion of this module, learners will have a comprehensive understanding of the NICE framework, security controls, networking concepts, traffic analysis, packet analyzers, sniffers, firewalls, SIEM, VLAN, VPN, identity and access management, and much more.

Domain 1 - Security Essentials

- Cybersecurity
- CIA Triad
- Malwares
- Attacks
- Threats
- Vulnerabilities
- Risk
- Security Controls

- BYOD
- NICE Framework
- Router
- Transmission media

Domain 2 - Network Basics

- Networking concepts
- OSI models
- TCP/IP model
- Ports
- Secure protocols
- Common network attacks
- Network Devices
- Hubs,
- Bridges
- Switch

Domain 3 - Network Security

- Security Devices
- Firewall
- Unified threat management (UTM)
- NGFW
- Web application firewalls
- Intrusion Detection Prevention System
- Network Access Control
- SIEM
- Secure Design
- Virtual Local Area Network (VLAN)
- Virtual Private Network (VPN)
- DMZ
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)

Domain 4 - Identity & Access Management

- AAA
- MFA
- Authorization
- Access control models
- IAM Lifecycle
- Authentication System
- SSO
- Active directory
- LDAP

Module 3 - Application and Web Application Security

The Application and Web Application Security course will enable learners to gain knowledge and skills in OWASP tools and methodologies, insecure deserialization, clickjacking, black box, white box, fuzzing, symmetric/ asymmetric cryptography, hashing, digital signatures, API security, patch management, and much more.

Domain 1 - Core Concepts

- Types of application
- Web application components
- Web servers
- Security policies, standards, procedures, guidelines, baselines

Domain 2 - Software Security

- Vulnerability database (VDB)
- SANS Top 25 Software Errors
- OWASP tools and methodologies
- Injection
- CSRF
- SSRF
- Clickjacking

Domain 3 - Secure Software Testing

- Vulnerability assessment
- Penetration testing
- SAST, DAST
- Black box, white box
- Fuzzing

Domain 4 - Cryptography

- Symmetric cryptography
- Asymmetric cryptography
- Hashing
- Digital Signature
- Digital Certificate
- Encryption
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security misconfigurations
- Cross site scripting (XSS)
- Insecure deserialization
- Using components with known
- vulnerabilities
- Insufficient logging and monitoring
- Beyond OWASP

Domain 5 - Secure Software Lifecycle Management

- SSDLC
- Threat modeling
- OWASP Secure coding guide
- API Security
- Common API Vulnerabilities
- How to stop API Attacks?
- System Hardening
- Secure configuration
- Patch management
- Application Monitoring & Logging

Module 4 - Ransomware and Malware Analysis

Malware, specifically ransomware, costs businesses more than $75 billion per year. These attacks continue to be a threat to the security of companies. In this module you will get an overview of how to detect, analyze, and protect yourself and your company from ransomware attacks.

Domain 1 - Introduction to Malware

- What is Malware?
- Malware Family
- History and Evolution of Malware
- What is Malware Market today
- Birth of a Malware
- Malware Distribution Technique
- How much damages malwares cause
- Is Ransomware a Malware
- Types of Ransomware
- How to defend Malware Infection
- Anatomy of a Ransomware Attack
- Ransomware Families
- Pros and Cons of Paying the Ransom
- Ransomware Operators and Targets
- How Does Ransomware Spread?
- Dealing with Ransomware Incidents
- Negotiate / Pay Ransom
- Ransomware threat prevention and response
- Secure Design Principles

Domain 2 - Malware Analysis

- What is malware analysis
- Why Malware Analysis
- Types of Malware analysis techniques
- Static analysis techniques
- Dynamic analysis techniques
- Malware Behaviors and Functionalities
- Malware Obfuscation Techniques

Domain 3 - Ransomware Malware

- Introduction to Ransomware
- Dangerous Convergences

Domain 4 - Advanced Malware Protection

- Enterprise Defense Strategies
- Protecting Endpoint
- Protecting Servers
- Zero-Trust Model
- Threat Intelligence and Malware Protection
- Ransomware Decryption Tools
- Ransomware Removal Tools
- The future of malware capabilities
- Future victims

Module 5 - Ethical Hacking and VAPT

This module provides you with the hands-on training required to master the techniques hackers use to penetrate network systems, helping you fortify your systems against it. You will also gain an understanding about the finer nuances of advanced hacking concepts, penetration testing, and vulnerability assessment.

Domain 1

- What is a Security Testing
- Why Security Testing
- What is a Security Vulnerability?
- Types of Security Testing
- Vulnerability Assessment
- Penetration Testing
- Breach Attack Simulation
- Manual and Automated Scanning
- Dealing with Vulnerabilities
- Types of Security Vulnerability
- National Vulnerability Database
- Selecting Technology

- Automation in VM
- Execution, Reporting, and Analysis
- Principles of Mitigation
- Exploitable Vulnerability Reporting
- Managing Vulnerabilities in the Cloud
- Vulnerability Remediation or Mitigation
- What is Vulnerability Management

Domain 2 - Vulnerability Assessment

- Vulnerability Assessment Program and
- Technology
- General Architecture
- Active and Passive Scanning Technology
- The Standard for Vulnerability Severity Rating
- Vulnerability database (VDB)
- Common Vulnerabilities and
- Exposures (CVE)
- Social Engineering
- Mobile Hacking
- Using the Metasploit Framework
- Exploitation
- Privileges Escalation
- Avoiding Detection
- Maintaining Access
- Covering your Tracks
- Cloud Penetration Testing

Domain 3 - Penetration Testing

- Penetration testing concepts i.e. what why & how we do pen test?
- Penetration testing methodology
- Types of penetration testing
- Tools and techniques used in penetration testing
- Information Discovery
- Scanning & Enumerating Target
- Introduction to Kali Linux
- System Hacking
- Infrastructure Hacking
- Client-Side Hacking
- Password Hacking
- Web Application Hacking

Domain 4 - Advanced Penetration Testing

- Red Teaming Operations
- Blue Teaming Operations
- Purple Teaming
- Breach Attack Simulation
- Bug Bounty Program
- Guidelines for Penetration Testers
- Being Ethical
- Gaining written permission
- Non-disclosure agreements
- Rules of engagement
- Penetration Testing Report Writing
- Report Read-Out

Module 6 - Capstone Project

This Capstone Project will allow you to implement the skills you learned throughout this program. Dedicated mentoring sessions will teach you how to solve a real-world, industry-aligned problem. This is the final step in the learning path and will enable you to showcase your expertise in cybersecurity to prospective employers.

Electives:

Module 1 - IIIT Bangalore Cybersecurity Master Class

Acquire a comprehensive understanding of technological advancements in cybersecurity through interactive masterclasses conducted by IIIT-B professors.

Module 2 - Masterclass by Former NPCI Expert

Attend online interactive masterclasses conducted by former NPCI expert and learn the practical application of acquired skills in Cybersecurity

Module 3 - Security Governance and Framework

Learn about the frameworks that govern the cybersecurity domain and the compliance requirements that professionals must follow in this field.

Module 4 - IBM: Network Security & Database Vulnerabilities

In this IBM module, you will understand TCP/IP and OSI models, DNS, DHCP, switching, routing, IP addressing, NAT, packet sniffing, and database vulnerabilities like SQL injection.

Module 5 - IBM: Penetration Testing, Incident Response and Forensics

In this IBM module, you will learn about pen testing tools for identifying security weaknesses, incident response techniques for effective handling of security incidents, the importance of digital forensics in investigations, and automation for increased efficiency and customization in cybersecurity operations.

Module 6 - Gen AI with Cybersecurity

Explore generative AI's critical role in cybersecurity, covering threat intelligence, report summarization, playbooks, and its impact on combating phishing, malware, misinformation, and deepfakes. Gain insights into cutting-edge strategies for cyber defense and threat prediction.

Capstone Projects

A day in the life of a
Security Analyst:

Review and update an organization's password policy settings to comply with the latest security requirements.

A day in the life of a
Malware Analyst:

Provide security to the bank's assets by examining, identifying, and understanding malware, such as viruses, worms, bots, rootkits, ransomware, and Trojan horse

A day in the life of a
Network Consultant:

Provide security to the bank's assets by designing, integrating, and implementing complex network architecture solutions after reviewing the network security.

A day in the life of a
Penetration Tester:

Run a gray-box penetration test using the tools at your disposal to probe for vulnerabilities that hackers with nefarious intent might be able to exploit to gather secure data.

Learning Outcomes

Upon successful completion of the program, you will:

1. **Proficient Understanding of NICE Framework:** Learners will demonstrate a comprehensive understanding of the NICE framework, enabling them to align cybersecurity practices with industry standards effectively.

2. **Expertise in Implementing Security Controls:** Learners will become adept at implementing various security controls to safeguard enterprise infrastructure, networks, and systems from cyber threats.

3. **Advanced Knowledge in Networking Concepts:** Learners will acquire advanced knowledge of networking concepts and their applications in enhancing security measures within organizational environments.

4. **Mastery of OWASP Tools and Methodologies:** Learners will master using OWASP tools and methodologies to identify and address vulnerabilities in web applications effectively.

5. **Capability to Secure APIs and Web Applications:** Learners will become proficient in securing APIs and web applications by adopting encryption techniques, patch management, and secure coding practices.

6. **Expertise in Ransomware Detection and Mitigation:** Learners will acquire specialized skills in detecting, analyzing, and mitigating ransomware attacks, contributing to heightened cybersecurity resilience for organizations.

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.

He did his M. Sc. (Engg.) at the Indian Institute of Science, Bangalore, India, between 2008-2011. He was affiliated to the Department of Computer Science & Automation. His thesis was supervised by Prof. Veni Madhavan. Prior to this, he obtained B. Tech. in Information Technology from National Institute of Technology Karnataka, Surathkal, India, in 2008.

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.

University Certificate

International Institute of Information Technology Bangalore

hereby confers upon

Jordan Smith

the

Advanced Executive Program in Cybersecurity

having successfully completed the requirements of the programme

(cohort start date: DD-MM-YYYY)

Prof. Debabrata Das
Director

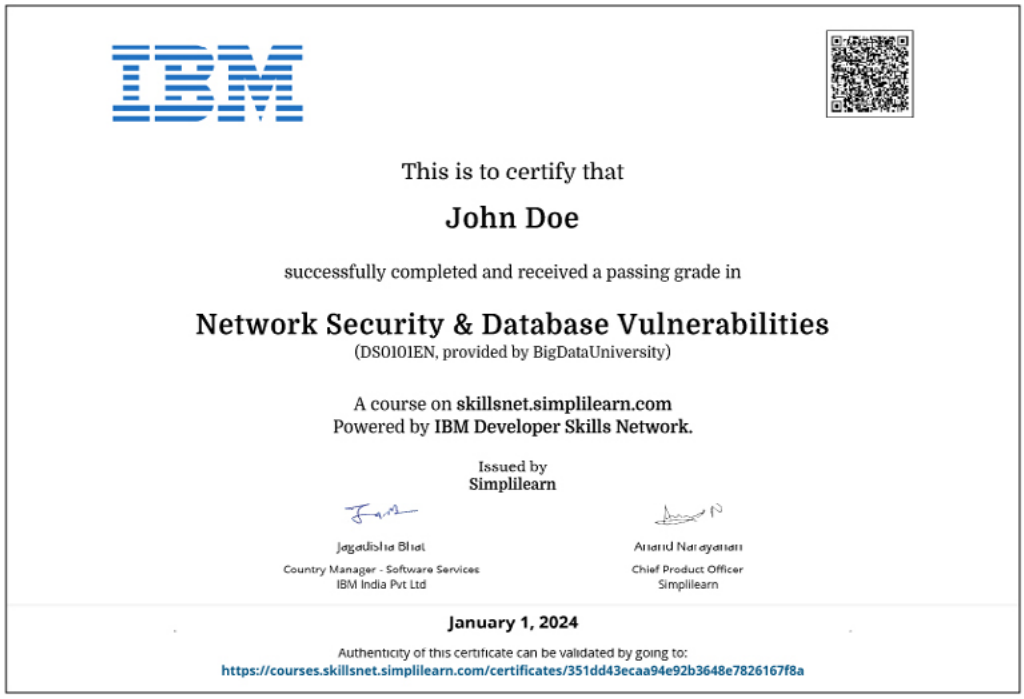
Cmde (Retd.) S R Sridhar
Registrar

Prof. Chandrashekar Ramanathan
Dean (Academics)

International Institute of Information Technology | 26/C, Electronics City, Hosur Road, Bengaluru 560 100 INDIA | http://www.iiitb.ac.in

Complete all the courses in the mandatory learning path successfully to obtain this industry-wide recognized course completion certificate from IIIT Bangalore.

IBM Certificate



This is to certify that

John Doe

successfully completed and received a passing grade in

Network Security & Database Vulnerabilities
(DS0101EN, provided by BigDataUniversity)

A course on **skillsnet.simplilearn.com**
Powered by **IBM Developer Skills Network.**

Issued by
Simplilearn

Jagadisha Bhat
Country Manager - Software Services
IBM India Pvt Ltd

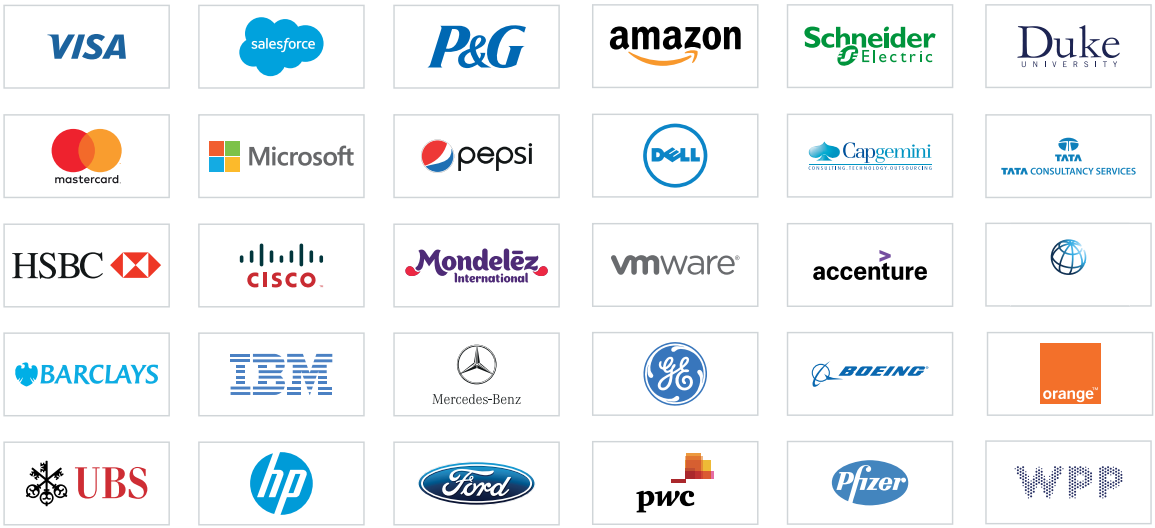
Anand Narayanan
Chief Product Officer
Simplilearn

January 1, 2024

Authenticity of this certificate can be validated by going to:
https://courses.skillsnet.simplilearn.com/certificates/351dd43ecaa94e92b3648e782167f8a

Industry-recognized IBM certificates for IBM courses

Corporate Training



Features of Corporate Training:

- Tailored learning solutions
- Flexible pricing options
- Enterprise-grade learning management system (LMS)
- Enterprise dashboards for individuals and teams
- 24X7 learner assistance and support

simplilearn

USA

Simplilearn Americas, Inc.
201 Spear Street, Suite 1100,
San Francisco, CA 94105
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

www.simplilearn.com