simplilearn

Advanced Executive Program in

Cybersecurity

Pioneering Excellence in Education, Research & Innovation

NPCI
भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

Table of Contents

About the Course

The digital landscape has grown by leaps and bounds. Cybersecurity skills are now among the most sought-after and highly-compensated skills 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.

Simplilearn's Advanced Executive Program in Cybersecurity, in collaboration with IIIT Bangalore and NPCI, will equip you with the skills necessary to transform your organization's cybersecurity strategy. You will learn comprehensive approaches to cryptography, API security, encryption, software security, network security, identity and access management, malware analysis, ransomware, vulnerability assessment, penetration testing, and much more.

In partnership with IIIT Bangalore and NPCI, this program features the perfect mix of theory, case studies, and extensive hands-on practical experience through integrated labs. The program provides a comprehensive education, leveraging IIIT Bangalore 's academic excellence, NPCI's expertise in secure retail and digital payments, and Simplilearn's unique blend of self-paced online videos, live virtual classes, hands-on projects, and integrated labs.

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 August 2021 edition and was ranked 10th in the same category as per India Today, August 2020 edition.

About NPCI

National Payments Corporation of India (NPCI), an umbrella organization for operating retail payments and settlement systems in India, is an initiative of the Reserve Bank of India (RBI) and the Indian Banks' Association (IBA), for creating a robust payment & settlement infrastructure in India. The corporation's current and future service portfolio includes Unified Payments Interface, RuPay, Immediate Payment Service, *99#, National Automated Clearing House, Aadhaar Enabled Payment System, e-KYC, Cheque Truncation System, National Financial Switch, etc.

About Simplilearn

Simplilearn is the world's #1 online bootcamp provider that enables learners through rigorous and highly specialized professional training programs. We focus on emerging technologies and processes that transform the digital world at a fraction of the cost and time as traditional approaches. Over two million professionals and 2,000 corporate training organizations have harnessed our award-winning programs to achieve their career and business goals.

Key Features

8X higher live interaction with live online classes by industry experts

Practice labs and projects with integrated labs

Program Completion Certificate from IIIT Bangalore

Virtual Internship Certificate from NPCI

Experiential learning via multiple real-life innovation projects and capstones

Lifetime access to self-paced videos & class recordings to refresh the concepts

Earn an industry recognized Simplilearn's Certificate after each module completion

Get noticed by the top hiring companies

Enrollment in Simplilearn's JobAssist (only for India)

Integrated Labs & Tools

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

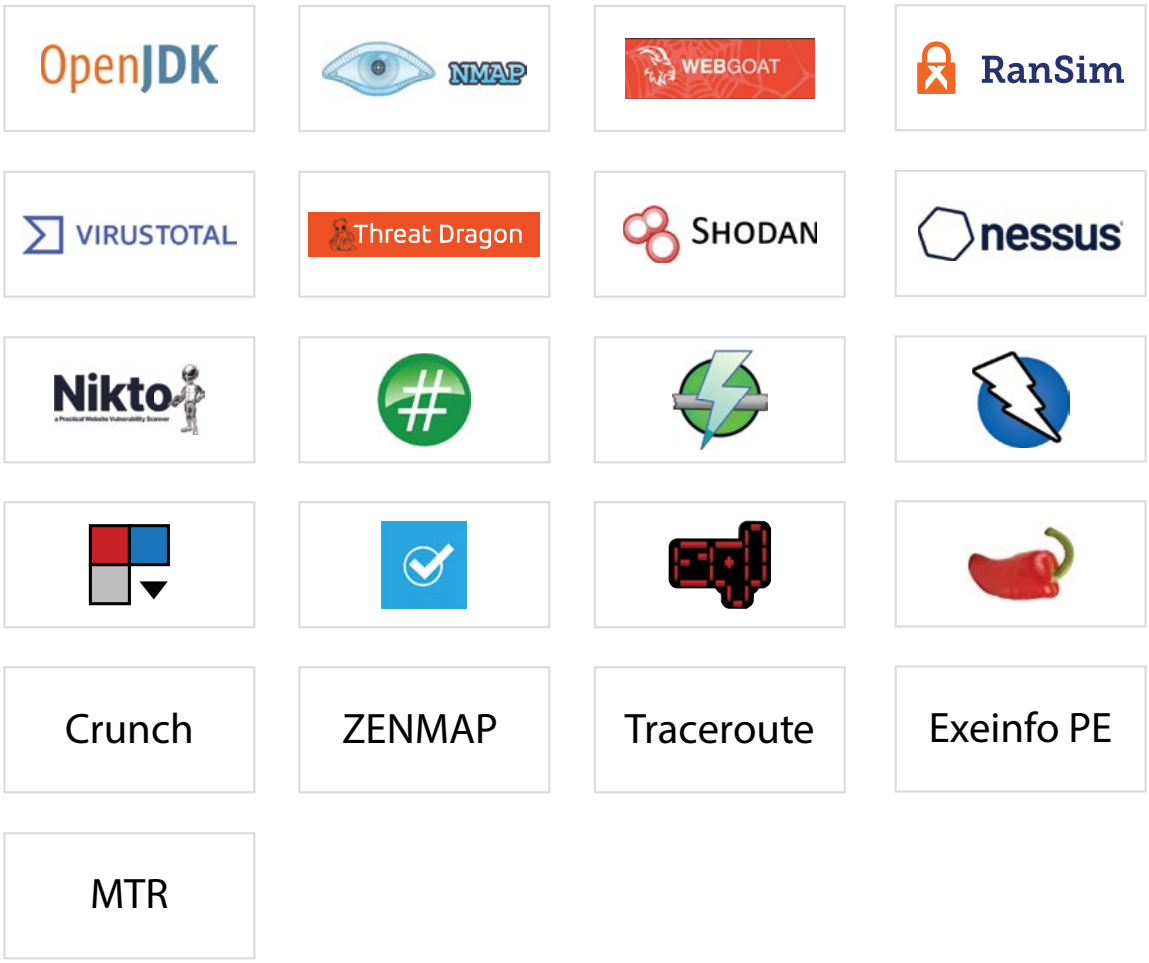
Windows OS

Kali Linux OS

Ubuntu OS

Webgoat

The malwares listed below are ones that a student would not want to install on his own computer, but with our labs VM, he can simply access them without causing harm to his PC.



Program Outcomes

At the end of this Advanced Executive Program in Cybersecurity, you will:

- Configure cybersecurity infrastructure components
- Learn fundamentals of cryptography and its application to network security
- Define the cybersecurity infrastructure policy or technical security policy for an organization
- Test and run exploits to identify vulnerabilities in networks
- Identify and analyze exposures and weaknesses in applications and their deployments
- Acquire a background on threat modeling, OWASP, fuzzing, clickjacking, etc.

Program Eligibility Criteria and Prerequisites

Those wishing to enroll in the Advanced Executive Program in Cybersecurity in collaboration with IIIT Bangalore and NPCI will be required to apply for admission.

Eligibility Criteria

For admission to this 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
- 1 year of work experience is mandatory

Application Process

The application process consists of three simple steps. An offer of admission will be made to the selected candidates and accepted by the candidates upon payment of the admission fee.

1

Submit an Application

Complete the application and include a brief statement of purpose to tell our admissions counselors why you're interested and qualified for this Advanced Executive Program in Cybersecurity.

2

Application Review

After you submit your application, a panel of admissions counselors will review your application and statement of purpose to determine your qualifications and interest in the program.

3

Admission

An offer of admission will be made to qualified candidates. You can accept this offer by paying the program fee.

Talk to an Admissions Counselor

We have a team of dedicated admissions counselors who are here to help guide you in the application process and related matters.

They are available to:

- Address questions related to the application
- Assist with financial aid (if required)
- Help you better understand the program and answer your questions

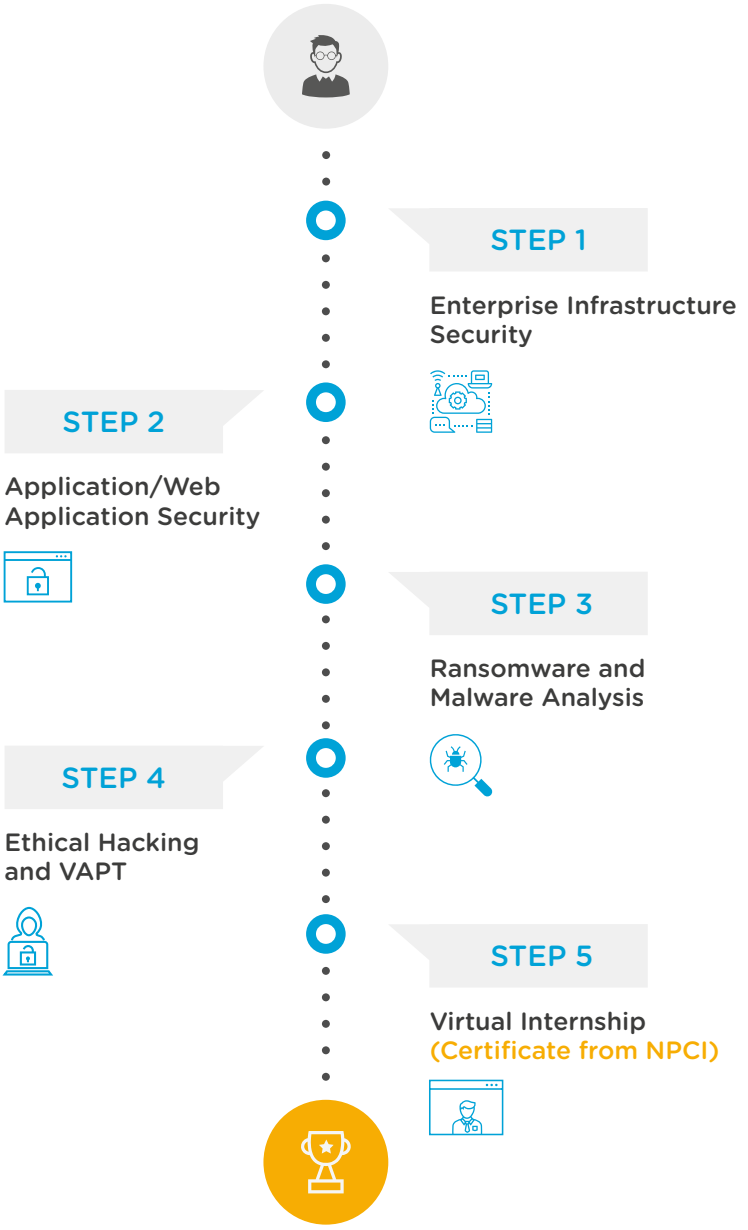
Who Should Enroll in this Program?

The program has been designed to meet the upskilling requirements of lower and mid-level management professionals working in BFSI, cybersecurity, and fintech fields who come with prior technical knowledge on 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: *We would be covering the basics of cybersecurity in our pre-requisite courses that would be assigned to the learners before the start of the program. Prior knowledge of any programming language is recommended but not mandatory.*

Learning Path



Advanced Executive Certificate in Cybersecurity from IIIT Bangalore

Electives

- Cloud Security (CCSP)
- Security Governance and Regulations

STEP 1 2 3 4 5

Enterprise Infrastructure Security

Module Overview:

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.

Module Curriculum:

Domain 1 - Security Essentials

- Cybersecurity
- CIA Triad
- Malwares
- Attacks
- Threats
- Vulnerabilities
- Risk
- Security Controls
- BYOD
- NICE Framework

Domain 2 - Network Basics

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

- Router
- Transmission media

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

STEP 1 2 3 4 5

Application and Web Application Security

Module Overview:

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.

Module Curriculum:

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
- 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

- 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

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

STEP 1 2 3 4 5

Ransomware and Malware Analysis

Module Overview:

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.

Module Curriculum:

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

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

- 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 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

STEP 1 2 3 4 5

Ethical Hacking and VAPT

Module Overview:

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.

Module Curriculum:

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
- 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)

- National Vulnerability Database
- Selecting Technology
- Automation in VM
- Execution, Reporting, and Analysis
- Principles of Mitigation
- Exploitable Vulnerability Reporting
- Managing Vulnerabilities in the Cloud

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
- Social Engineering
- Mobile Hacking
- Using the Metasploit Framework
- Exploitation
- Privileges Escalation
- Avoiding Detection
- Maintaining Access
- Covering your Tracks
- Cloud Penetration Testing

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

STEP 1 2 3 4 **5**

Virtual Internship

This virtual internship will give you an opportunity to implement the skills you learned throughout this program. Through dedicated mentoring sessions, you will learn 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.

Advisory Board Member

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, IT and ITeS Sectional Committee, Services Sector Department 10, Bureau of Indian Standards, June 2020 – Current.
- Member, Technical and Financial Advisory Committee, E-Procurement, Centre for E-Governance, Government of Karnataka. Apr 2019-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)

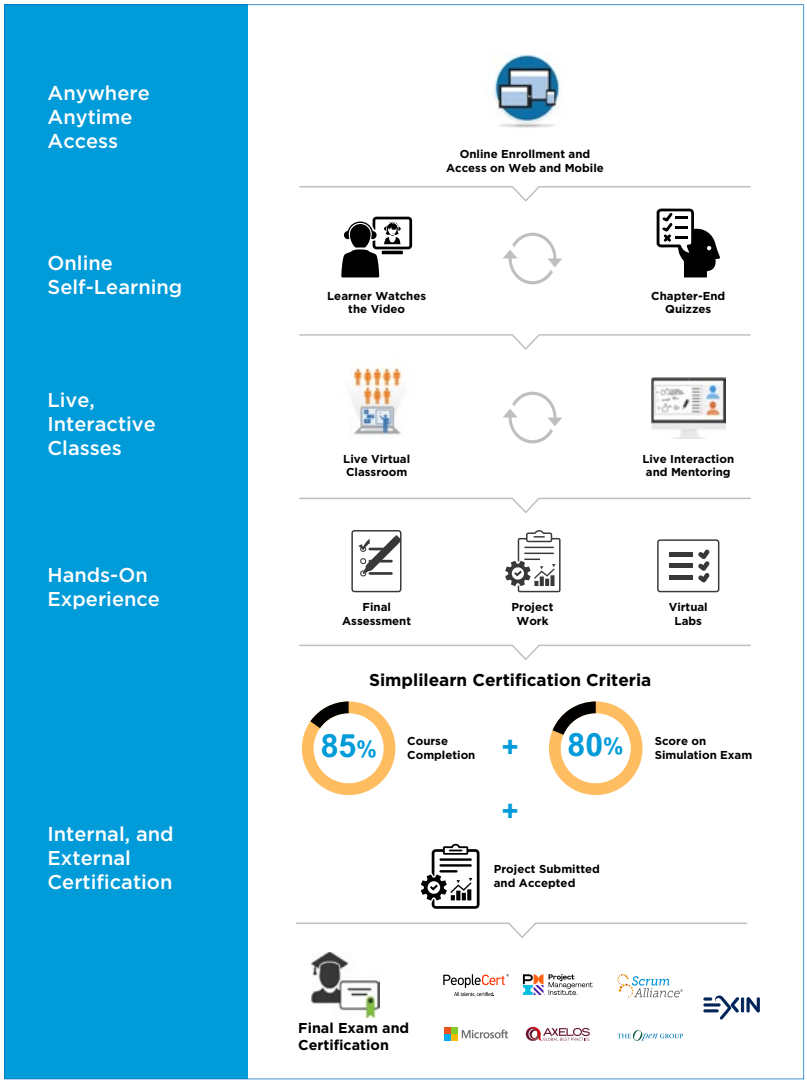
Professor Chandrashekar Ramanathan is a faculty member at IIITB since 2007. Professor Chandrashekar received his Ph.D degree from Mississippi State University. His thesis was in the area of object-oriented databases. He has extensive application software development experience spanning over 10 years 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.

Certificate

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

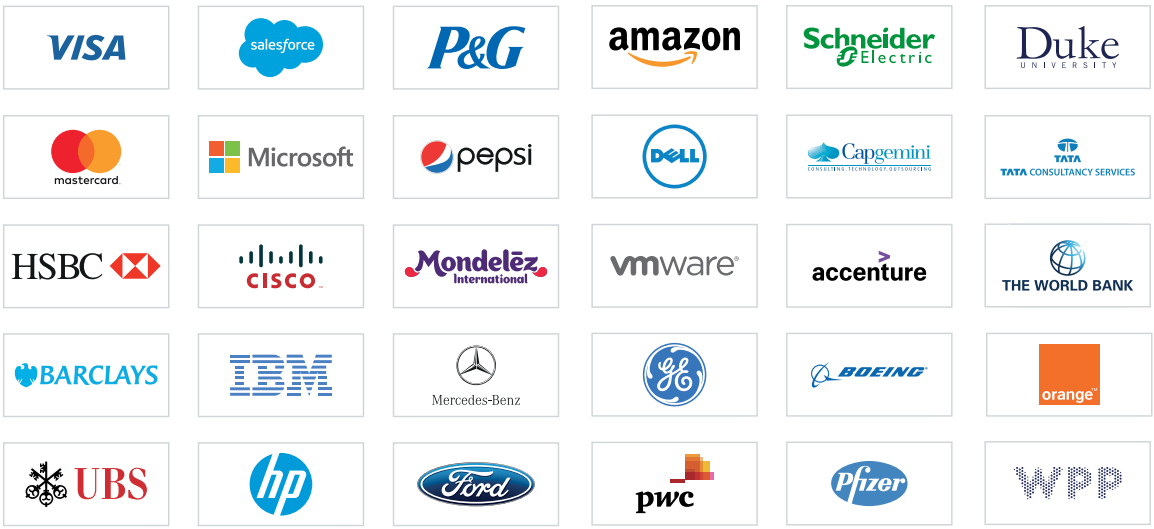
When you have achieved this Certification, you acquire the necessary skills helping you to stay competitive in the cybersecurity industry. The certification proves to be a testimonial that you have gained in-depth knowledge of the underlying technology needed to perform the tasks efficiently in your job.

Classroom-Level Immersion: Delivered Digitally



Corporate Training

Top clients we work with:



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

INDIA

Simplilearn Solutions Pvt Ltd.

53/1 C, Manoj Arcade, 24th Main,
Harlkunte
2nd Sector, HSR Layout
Bangalore - 560102

Call us at: 1800-212-7688

USA

Simplilearn Americas, Inc.

201 Spear Street, Suite 1100,
San Francisco, CA 94105
United States

Phone No: +1-844-532-7688

www.simplilearn.com