

Executive Certification in **Cyber Security &** **Ethical Hacking**

In collaboration with



Program designed for IT professionals



Table Of Content

1	How to make an Impact
2	Program Summary
3	About Course
4	Who is this program for?
5	Why choose Learnbay?
6	Others Vs Learnbay
7	Alumni Spotlight
8	Certification
9	Fee & Batch Details
10	Program Curriculum

How to make an
impact with



iHUB DivyaSampark
IIT Roorkee



*Designed for **IT professionals, network administrators**, and security analysts, this program equips you with the expertise to excel and lead in the ever-evolving **Cybersecurity domain**.*



Real-World Project Experience

Build end-to-end Cyber Security projects with practical hands-on training.



Certification from iHUB DivyaSampark, IIT Roorkee

Receive a prestigious completion certificate from **iHUB DivyaSampark, IIT Roorkee**.



Immersive Experience

2-day classroom learning at IIT Roorkee from IIT professionals.



Master Cybersecurity Tools

Learn **IAM, ISO Standard** with end-to-end real projects.

Program **Summary**



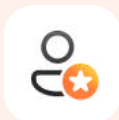
Program Eligibility

Working professionals having **minimum 1** years of exp.



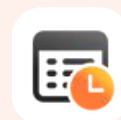
Training Mode

100% Instructor led
Live Online sessions



Program Faculty

Industry Experts and
iHUB DivyaSampark, IIT Roorkee Professors



Program Duration

8 Months Program
Weekday and Weekend
Batch



Payment Options

No cost EMI,
Interest free loan



Certification

From **iHUB**
DivyaSampark, IIT Roorkee

Exclusive

Master **GenAI** **Skills** for Cyber Security

GenAI Projects

Work on GenAI Projects
designed for Security eng

Practical Skills

Gain hands-on experience
in Cyber Security

Dedicated Mentors

Dedicated projects
mentors from industry

Industry Knowledge

Develop expertise in
your specific domain.

Important Note: Gain real project experience in Cybersecurity under the guidance of industry mentors. Work with a team to **implement projects** with Generative AI applications.

About Course

This program is designed for **IT professionals**, security analysts, and cybersecurity practitioners to advance their skills through **project-based learning** guided by industry mentors.

It integrates **Generative AI** into Cybersecurity, covering threat detection, vulnerability assessment, incident response, and security automation. By the end, you'll be ready to tackle **real-world challenges** and excel in high-demand cybersecurity roles.

Our Commitment

Empower tech professionals and security enthusiasts to excel in **Cybersecurity and Generative AI** by mastering key concepts, practical applications, and tools for effective threat management and decision-making.

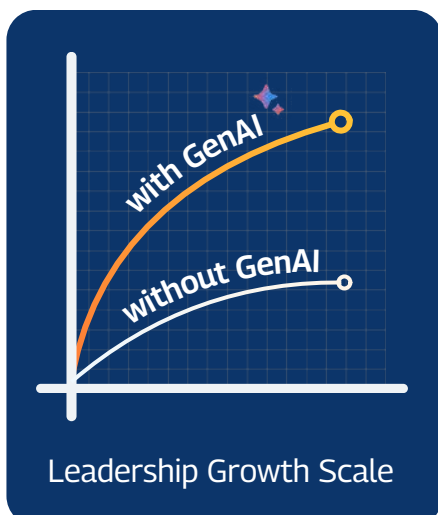
Additionally, our career support services include **interview preparation, resume building, and job placement assistance**, ensuring a smooth transition into high-demand roles in Cybersecurity and Generative AI.

 **100%**
Assured Interview

 **350+**
Hiring Partners

 **7+**
Centers Across India

 **40k+**
Professionals Upskilled



82%

of Security eng are likely to adopt GenAI by 2025, to


- enhance efficiency,
- automating tasks,
- improving decision-making for better project outcomes.


***By integrating GenAI into our programs**, we ensure that our learners are well-prepared to lead and innovate in their respective fields.



Who is this program for?

A unique program For IT
Professionals & Engineers

 www.learnbay.co

 77956 87988

Entry to Mid Level Professionals with **1+ Years of Experience**

This program is perfect for Security Analysts, Risk Consultants, Compliance Officers, Entrepreneurs, and Network Administrators.



IT/Tech Professionals



IT/System Admin

Important Note: This program is not for freshers, fresh grads, students.

Program Outcome: What's in it for you?



Industry Recognized Cybersecurity Certification

Learn Cybersecurity and Ethical Hacking with real-world projects. Mastering these skills helps to protect and secure system against threats.



Master GenAI Skills for Cybersecurity

By integrating GenAI into our programs, we ensure that our learners are **well-prepared to lead** and innovate in their respective fields.



Accelerate Your Career Growth


Leverage advanced GenAI knowledge to drive business success, enhancing career prospects and **salary growth**.



Why choose Learnbay?

A unique program For IT
Professionals & Engineers

 www.learnbay.co

 77956 87988

Why choose Learnbay?

For Executive Certification in Cyber Security



iHUB DivyaSampark, IIT Roorkee Certification

Stand out with a prestigious certification from **iHUB DivyaSampark, IIT Roorkee**.

Get Certified
from



Project-Based Learning

Gain hands-on experience with **real-world Cyber Security projects**, preparing you to tackle industry challenges.

Real Projects | Real Experience



Learn from Industry Mentors

Gain insights from top industry experts in Cyber Security. Our mentors bring **real-world experience** to help you master advanced skills.



Personalized Support

Get tailored guidance with **1:1 doubt-clearing sessions** for a deeper understanding.

Others Vs Learnbay

 Learnbay

OTHERS

Training Mode



100% Online & Hybrid
(Online + Classroom)



Only recorded class
& few live online

Support



24/7 Student
Support



Limited Support
Hours

Placement



100% Placement
Assistance



Limited Placement
Support

Curriculum



Included in Latest
Curriculum



Often Not Included

Faculty



Experienced Industry
Professionals



Academics and
Trainers

Real-Time
Projects



Practice with Live
Projects and Team
Management



Simulated Projects

Get certified

and accelerate your career growth

iHUB DivyaSampark, IIT Roorkee.



Certification from iHUB DivyaSampark, IIT Roorkee

- ✓ Executive Certification: Earned in Cyber Security from ihub DivyaSampark, IIT Roorkee.
- ✓ Hands-On Experience: Practical learning at IIT Roorkee campus.
- ✓ Top Faculty: Learn directly from IIT experts.

Certified Ethical Hacker



EC Council Certified ethical hacker Certificate

Gain an internationally recognized EC-Council certificate, Worlds No. 1 Credential, to build your cyber career

Program Fees

Live online classes

- ✓ Live online interactive sessions
- ✓ 1:1 online Doubt Session with experts
- ✓ Virtual Mock interviews
- ✓ Online Capstone projects

Program Fee

₹ 1,10,000

Pay in easy EMIs starting as low as

₹ 7,211/ month


Tools and Modules






Program Curriculum

A unique program For IT
Professionals & Engineers

 www.learnbay.co

 77956 87988

TERM 1

Fundamentals and Prerequisites

Duration: 50 Hours

Outcome of this term: This term builds foundational skills in OS, networking, and cloud security, with hands-on practice using Kali Linux and key cybersecurity tools.

Module 1: Operating System Basics

- **Windows** and **Linux** OS Fundamentals
- User and Access Permissions
- OS Hardening Techniques
- Introduction to Virtualization and Setting Up Virtual Labs (**Kali** Linux Installation and Usage)

Module 2: Networking Fundamentals

- **Network Topologies** and Protocols (OSI and TCP/IP Models)
- **IP Addressing**, Subnetting, and Routing Basics
- Network Devices: Routers, Switches, Firewalls, **Load Balancers**
- VPNs, **Proxy Servers**, and Network Security

Module 3: Cloud Security Basics

- Cloud Computing Models (**IaaS, PaaS, SaaS**)
- Shared Responsibility Model in Cloud
- Basic Cloud Security Controls
- **Hands-On: Setting up a Secure Cloud Instance**

Module 4: Introduction to Kali Linux and Security Tools

- Overview of Kali Linux Environment
- Basic Commands and Utilities in Kali Linux
- Introduction to Security and Hacking Tools (**Nmap, Wireshark, Metasploit**)
- **Hands-On Lab: Basic Scanning and Enumeration**

TERM 2

Ethical Hacking and Penetration Testing

Duration: 45 Hours

Outcome of this term: This term introduces ethical hacking, focusing on reconnaissance, social engineering, and network scanning techniques. You'll gain hands-on experience with tools like Nmap and Wireshark to analyze and secure networks effectively.

Module 1: Introduction to Ethical Hacking

- Overview of **Ethical Hacking** and Cybersecurity
- Understanding **Cyber Attack Vectors**
- Hacking vs. Ethical Hacking: Ethics and Legal Aspects
- **Key Phases of Hacking:** Reconnaissance, Scanning, Exploitation, and Covering Tracks

Module 2: Footprinting, Reconnaissance, & Social Engineering Attacks

- Techniques for Information Gathering (Passive and Active)
- **Social Engineering Attacks:** Phishing, Pretexting, Baiting
- **Phishing Techniques** and Tools (SET, Social-Engineer Toolkit)
- **Hands-On Project: Conducting Reconnaissance and Simulating a Phishing Attack**

Module 3: Network Scanning and Enumeration

- Network Scanning Techniques and Tools (**Nmap, Netcat**)
- Enumeration of Network Services and Devices
- **Hands-On Project: Scanning a Network and Enumerating Hosts and Services**

Module 4: Sniffing and Traffic Analysis

- Basics of Sniffing and Importance of **Traffic Analysis**
- Types of Sniffing: Active vs. Passive
- **Hands-On Project: Capturing and Analyzing Network Traffic with Wireshark**

TERM 3

Advanced Cybersecurity Techniques

Duration: 35 Hours

Outcome of this term: This term covers vulnerability assessment, malware analysis, and web application security. You'll gain practical skills in tools like Nessus, Burp Suite, and OWASP ZAP to identify and mitigate threats.

Module 1: Vulnerability Assessment and Denial-of-Service (DoS) Attacks

- Vulnerability Assessment Techniques and Tools (**Nessus, OpenVAS**)
- Types of Denial-of-Service (**DoS**) and Distributed DoS (DDoS) Attacks
- **Hands-On Project: Conducting a Vulnerability Assessment and Simulating a Basic DoS Attack**

Module 2: System Hacking, Privilege Escalation, & Session Hijacking

- System Hacking Techniques and **Privilege Escalation**
- Password Cracking Tools (Hydra, John the Ripper)
- **Evading Security Measures:** Bypassing IDS, Firewalls, and Honeypots

Module 3: Malware Threats and Protection

- Types of Malware: **Viruses, Worms, Trojans, Ransomware**
- Malware Analysis Techniques and Tools
- Methods to Protect Against Malware Attacks

Module 4: Web Server & Application Hacking

- **Common Web Vulnerabilities:** SQL Injection, XSS, CSRF
- Web Application Security Testing Tools (**Burp Suite, OWASP ZAP**)
- **Hands-On Project: Testing Web Applications for SQL Injection and XSS Vulnerabilities**

TERM 4

Cybersecurity and Information Security Essentials

Duration: 35 Hours

Outcome of this term: This term provides a strong foundation in cybersecurity principles, frameworks, and network security. You'll learn incident response and forensics through hands-on labs, preparing you to address real-world cyber threats.

Module 1: Cybersecurity Basics and Fundamentals

- **Core Principles:** Confidentiality, Integrity, Availability (CIA Triad)
- Key Cyber Threats: Malware, Phishing, Ransomware
- Overview of Cybersecurity Domains (**Network, Application, Cloud, Data**)

Module 2: Cybersecurity Frameworks & Compliance Standards

- Introduction to Cybersecurity Frameworks (**NIST, ISO 27001**)
- Key Compliance Standards: **GDPR, PCI-DSS**, and India-Specific Laws (**IT Act**)
- Implementing Security Policies and Risk Management in Organizations

Module 3: Network Security Essentials

- Basics of Firewalls, **VPNs, IDS/IPS**
- Network Security Best Practices for Small and Large Businesses
- **Hands-On Lab: Configuring Firewalls and VPN Connections**

Module 4: Incident Response and Forensics

- Steps in Incident Response (**Preparation, Detection, Containment, Recovery**)
- Basics of Digital Forensics and Evidence Handling
- **Hands-On Lab: Simulating a Security Incident and Conducting Basic Forensics**

TERM 5

Advanced Cybersecurity and Threat Intelligence

Duration: 35 Hours

Outcome of this term: This term focuses on cloud security, IAM, and advanced cyber threat intelligence, equipping you with skills to secure systems. Specialized electives offer insights into niche areas like IoT, Red Teaming, and automation.

Module 1: Cloud Security and IAM

- Understanding **Cloud Models** (Public, Private, Hybrid)
- Shared Responsibility Model and Cloud **Threats**
- Basics of IAM (Identity and Access Management) for Cloud Security
- **Hands-On Lab: Securing a Cloud Environment and Configuring IAM**

Module 2: Identity and Access Management (IAM) & Endpoint Security

- Role-Based Access Control (**RBAC**) and Multi-Factor Authentication (MFA)
- Endpoint Security Best Practices (**Antivirus, Patching**)
- **Hands-On Lab: Setting Up IAM Controls and Configuring Endpoint Protection**

Module 3: Advanced Cyber Threats and Threat Intelligence

- Advanced Persistent Threats (**APT**) and Ransomware
- Cyber Threat Intelligence: Indicators of Compromise (**IoCs**)
- **Hands-On Lab: Setting Up Basic Threat Detection and IoC Analysis**

Module 4: Specialization Electives

- Mobile and IoT Security
- **Red Teaming** and **Blue Teaming** Basics
- Industrial Cybersecurity
- Cybersecurity Automation

TERM 6

Generative AI in Cybersecurity

Duration: 30 Hours

Outcome of this term: This term explores Generative AI applications in cybersecurity, focusing on threat detection, incident response automation, and malware analysis. You'll gain hands-on experience building GenAI models for real-world security challenges.

Module 1: Introduction to Generative AI in Cybersecurity

- Basics of Generative AI and Its Role in Cybersecurity
- **Applications: Threat Detection, Automated Response, and Malware Analysis**

Module 2: Generative AI for Threat Detection

- Detecting Network **Anomalies** with GenAI
- **Hands-On Lab: Developing a Simple GenAI Model for Detecting Unusual Network Activity**

Module 3: Incident Response Automation with Generative AI

- How GenAI Automates Security Alerts and **Incident Response**
- **Hands-On Lab: Building a GenAI-Based Chatbot for Incident Response**

Module 4: GenAI for Malware and Phishing Detection

- Using AI to Detect **Malware** Patterns and Identify **Phishing** Attempts
- **Hands-On Lab: Using GenAI to Detect Phishing and Analyze Malware Samples**

Executive-level real-time **Industrial Projects**

#1

Zero Trust Security Framework

Design and deploy a zero trust security framework to restrict access based on verified identity and continuous authentication.

Tools: Okta, Azure AD, AWS IAM, Palo Alto Prisma

Outcome: Implement a robust security model ensuring secure resource access.

#2

AI-Powered Threat Detection System

Build an AI-driven system to detect and analyze threats using anomaly detection and predictive models for proactive defense.

Tools: TensorFlow, Keras, ELK Stack, Splunk

Outcome: Deliver a system that identifies and mitigates cyber threats in real time.

#3

Web-Based Facial Authentication System

Develop a facial recognition system to authenticate web users securely by leveraging advanced AI algorithms for real-time validation.

Tools: OpenCV, Azure Cognitive Services, TensorFlow, AWS Rekognition

Outcome: Enhance web security with an accurate and user-friendly authentication tool.

#4

Multi-Factor User Authentication System

Create a multi-factor authentication system combining biometrics, OTPs, and passwords for comprehensive user access security.

Tools: Twilio, Google Authenticator, OpenID

Outcome: Provide a layered security approach for secure and reliable user logins.

Thank you!

For more queries and information
please reach out to us at:

+91 77956 87988

Visit us at

www.learnbay.co

