

# POST GRADUATE CERTIFICATION PROGRAM IN CYBER SECURITY



**Electronics & ICT Academy**  
Indian Institute of Technology Guwahati  
An Initiative of Ministry of Electronics & Information Technology(Meity)

 **Duration: 12 Months**

In association with



# INDEX

About the Program	01
About E&ICT Academy	02
Adout Securium Academy	03
Eligibility Criteria	04
Timescale	04
Future Job Roles after this Program Key Learning Outcomes	05-07
How to Apply	13
Who's this program is for?	13
Pre-Requisites	14
CORE TOPICS	15-19
Course Fees	19
Virtual Environment and Distributions Tools	20
Learning Outcomes	21
Career Support	22
Certificate	23
Corporate Internship Opportunity	24

# About The Program

The "POST GRADUATE CERTIFICATION PROGRAM IN CYBER SECURITY" is an intensive and comprehensive training initiative conducted by Securium Solutions Private Limited [Securium Academy], in partnership with E&ICT Academy, IIT Guwahati. This prestigious program is designed to equip students with advanced skills and knowledge in the critical areas of Web Application, Network and Mobile Application

penetration testing, Security Operation Center, Incident Handling, Computer Forensics and Compliance Auditing. Through a rigorous curriculum, participants will delve into the principles of Penetration Testing, Incident Handling, learn the latest techniques in Penetration Testing, and master the tools and methodologies essential for effective penetration testing and Incident handling along with Forensics and Compliance.

The program stands out by offering an E&ICT Academy, IIT Guwahati certification, a credential that holds significant value and recognition in the industry.

This collaboration ensures that the training meets the highest educational standards and is delivered by experts in the field. Participants will benefit from a blend of theoretical knowledge and practical application, preparing them to tackle real-world cybersecurity challenges.

Upon successful completion of the program, students may also have the opportunity to secure internships with Securium Solutions Private Limited. These internships provide invaluable hands-on experience, allowing students to apply their learning in real-world scenarios, work alongside seasoned professionals, and gain a deeper understanding of the cybersecurity landscape. This Post Graduate Certificate program not only enhances students' technical skills but also significantly boosts their career prospects, making them highly competitive candidates in the rapidly growing field of cybersecurity.





# Electronics & ICT Academy

Indian Institute of Technology Guwahati

An Initiative of Ministry of Electronics & Information Technology(Meity)

## About Electronics and ICT Academy

The Ministry of Electronics and Information Technology initiated the Electronics and ICT Academy (E&ICT Academy) to boost digital proficiency among students and professionals. Set up in collaboration with premier institutes including IITG, the academy provides quality education via assorted training, workshops and certifications.

It addresses skill gaps in emerging technologies such as AI, machine learning and IoT. Industry collaborations help match training with market needs. The E&ICT Academy IIT Guwahati plays a key role in readying a technically-skilled workforce for the rapidly evolving digital landscape by bridging demand and supply gaps.



# About Securium Academy

Securium Academy operating under the brand name Securium Solutions Private Limited, is a leading pioneer in the field of cybersecurity services and consulting. Renowned for its commitment to excellence and innovation, Securium Solutions offers a comprehensive range of cybersecurity solutions designed to protect organizations from evolving digital threats. The company specializes in services such as ethical hacking, penetration testing, vulnerability assessments, security audits, and incident response, catering to clients across various industries.

Securium Academy, the educational arm of Securium Solutions, is dedicated to empowering individuals and organizations with the knowledge and skills needed to navigate the complex world of cybersecurity. By providing cutting-edge training programs and certifications, Securium Academy aims to bridge the gap between theoretical knowledge and practical application. Their programs are crafted by industry experts and cover a wide spectrum of cybersecurity topics, ensuring that participants are well-equipped to meet the demands of the ever-changing digital landscape.

Partnering with prestigious institutions like E&ICT, IIT Guwahati and Securium Academy offers top-tier training opportunities that combine academic rigor with real-world relevance. These collaborations not only enhance the quality of the educational experience but also provide participants with credentials that are highly respected in the industry. Through its comprehensive training programs, hands-on learning approach, and strong industry connections, Securium Solutions Private Limited [Securium Academy] is committed to shaping the next generation of cybersecurity professionals and leaders.



# Eligibility Criteria

To Apply, Candidates should meet the criteria of



Would have graduated a bachelor's degree or Master's degree with 50% Marks minimum..



No Need of any prior Experience



No need of Programming Languages at this level

## Timescale

- ✓ 250+ hours of Live Online Training
- ✓ 125 Sessions
- ✓ Duration: 12 Months

## Highlights

- ✓ 12 Months Curriculum covering End-to-End Cyber Security Concepts Live
- ✓ Online learning with Industry Experts
- ✓ Variable Work Schedule
- ✓ Alumni Status of E&ICT Academy IIT Guwahati

# Future Job Roles after this Program

Completing a "POST GRADUATE CERTIFICATION PROGRAM IN CYBER SECURITY from Securium Solutions in partnership with E&ICT Academy IIT Guwahati can open up various advanced job roles in the cybersecurity field. Here are some potential job roles you could pursue:



## **Penetration Tester :**

Conduct simulated attacks on networks, applications, and systems to identify vulnerabilities.

Provide detailed reports and recommendations for improving security posture.



## **Security Operations Center (SOC) Analyst:**

Monitor and analyze security incidents in real-time.

Respond to and mitigate threats as they occur.

## **Incident Responder:**



Act swiftly to address security breaches and mitigate damage.

Conduct thorough investigations and develop response plans.

## **Digital Forensics Analyst:**



Investigate cybersecurity by analyzing digital evidence. Work with law enforcement and legal teams to support investigations and prosecutions.



**Compliance Auditor:** Ensure the organization complies with relevant laws and regulations.

Conduct audits and assessments to identify gaps and recommend improvements.



## **Network Security Engineer:**

Design and implement secure network infrastructures.

Monitor network traffic for suspicious activity and implement protective measures.

# Future Job Roles after this Program



## **Application Security Specialist:**

Focus on securing web and mobile applications.

Conduct code reviews, penetration tests, and implement security best practices.



## **Cybersecurity Consultant:**

Provide expert advice and solutions to organizations on improving their security posture.

Conduct risk assessments, develop security policies, and design security architectures.



## **Threat Intelligence Analyst:**

Analyze threat data and provide insights on potential risks to the organization.

Develop strategies to mitigate identified threats.



## **Digital Forensics Analyst:**

Investigate cybercrimes by analyzing digital evidence.

Work with law enforcement and legal teams to support investigations and prosecutions.



## **Compliance Auditor:**

Ensure that organizations comply with relevant laws and regulations

Conduct audits and assessments to identify gaps and recommend improvements.



## **Network Security Engineer:**

Design and implement secure network infrastructures.

Monitor network traffic for suspicious activity and implement protective measures.



## **Security Architect:**

Design and implement comprehensive security solutions for organizations

Ensure that security measures are integrated into all aspects of IT infrastructure.



# Future Job Roles after this Program



## **Chief Information Security Officer (CISO):**

lead an organization's cybersecurity strategy and operation.

Develop and implement policies and procedures to protect the organization's information assets



## **Computer and Information Systems Manager**

Oversee the IT department, ensuring that systems are secure and running efficiently.

Implement and manage security measures across the organization.



## **Vulnerability Analyst/Researcher:**

identify and research potential security vulnerabilities in software hardware

work on developing and apply patches or mitigation techniques



## **Cloud Security Engineer:**

Focus on setting cloud- based system and data.

implement security measures and conduct regular audits of cloud environments.



## **Risk Manager:**

Identify , assess and mitigate risks to the organization's information systems.

Develop risk management strategies and policies

# Key Learning Outcomes

- ✓ Advanced Understanding of Cyber security Principles
- ✓ Expertise in Web Application Security
- ✓ Proficiency in Network Security
- ✓ Specialized Skills in Mobile Application Security:
- ✓ Operational Skills in Security Operations Center (SOC):
- ✓ Competence in Incident Handling and Response:
- ✓ Digital Forensics Proficiency:
- ✓ Knowledge of Compliance and Auditing:
- ✓ Mastery of Security Tools and Methodologies:
- ✓ Ability to Detect and Mitigate Advanced Threats:
- ✓ Hands-On Experience through Labs and Projects:
- ✓ Enhanced Critical Thinking and Problem-Solving Skills:
- ✓ Improved Collaboration and Communication Skills:
- ✓ Awareness of Latest Trends and Technologies:
- ✓ Understanding of Ethical and Legal Aspects:
- ✓ Preparation for Advanced Cybersecurity Roles:
- ✓ Campus immersion programme at EICT Academy IIT Guwahati (only for successful learners)



## Web Penetration Testing

- ✓ Understanding Web Application Architectures
- ✓ Familiarity with Common Web Vulnerabilities
- ✓ Proficiency with Web Penetration Testing Tools
- ✓ Knowledge of Authentication and Authorization Mechanisms
- ✓ Experience with Manual Testing Techniques
- ✓ Report Writing Skills



## Network Penetration Testing

- ✓ Understanding Network Architectures and Protocols
- ✓ Knowledge of Network Vulnerabilities
- ✓ Proficiency with Network Penetration Testing Tools
- ✓ Experience with Network Attack Techniques
- ✓ Understanding of Firewall and IDS/IPS Evasion Techniques
- ✓ Report Writing Skills





## Mobile Penetration Testing (Android & iOS)

- ✓ Understanding Network Architectures and Protocols
- ✓ Knowledge of Network Vulnerabilities
- ✓ Proficiency with Network Penetration Testing Tools
- ✓ Experience with Network Attack Techniques
- ✓ Understanding of Firewall and IDS/IPS Evasion Techniques
- ✓ Report Writing Skills



## Incident Handling

- ✓ Understanding Incident Response Life Cycle
- ✓ Incident Detection and Analysis
- ✓ Effective Incident Response Planning
- ✓ Containment Strategies
- ✓ Eradication and recovery Techniques
- ✓ Communication and coordination
- ✓ Legal and Regulatory Considerations
- ✓ Forensic Analysis
- ✓ Incident Reporting and Documentation



## Incident Handling

- ✓ Post-Incident Activities
- ✓ Use of Incident Response Tools
- ✓ Development of a Security Incident Response Team (SIRT)
- ✓ Continuous Improvement in Incident Handling
- ✓ Real-World Incident Handling Scenarios



## Computer Forensics:

- ✓ Understanding Digital Foren
- ✓ Understanding Digital Forensics Principles
- ✓ Knowledge of Forensic Tools and Techniques
- ✓ Evidence Collection and Preservation
- ✓ Forensic Analysis of Digital Devices
- ✓ File System Forensics
- ✓ Network Forensics
- ✓ Malware Analysis
- ✓ Incident Response and Forensics Integration
- ✓ Legal and Ethical Considerations
- ✓ Report Writing and Documentation
- ✓ Forensic Investigation of Cybercrimes
- ✓ Real-World Forensic Scenarios
- ✓ Advanced Forensic Techniques
- ✓ Development of Analytical and Critical Thinking Skills
- ✓ Understanding of Forensic Standards and Best Practices
- ✓ Collaboration with Law Enforcement and Legal Teams



## Compliance

- ✓ Understanding of ISO 27001 Standard
- ✓ Knowledge of Information Security Management Systems (ISMS)
- ✓ Risk Assessment and Management
- ✓ Compliance Auditing Techniques
- ✓ Internal Audit Process
- ✓ Gap Analysis
- ✓ Understanding of ISO 27001 Certification Process:
- ✓ Audit Reporting and Documentation
- ✓ Legal and Regulatory Compliance
- ✓ Continuous Improvement:
- ✓ Stakeholder Communication
- ✓ Practical Audit Experience:
- ✓ Awareness of Best Practices and Industry Standards:
- ✓ Development of Analytical and Critical Thinking Skills
- ✓ Preparation for Professional Certification:



## Cross-Discipline Learning Outcomes

- ✓ Analytical and Critical Thinking Skills
- ✓ Problem-Solving Skill
- ✓ Ethical Hacking Principles
- ✓ Continuous Learning

# How to Apply



## Application Submission

Apply for the program by completing the application with one page cover letter stating your Interest and Qualifications for the program.



## Application Review

Admission Counselors will review applications and cover letter to Qualify your Application



## Admission

Candidates admission will be confirmed by paying the program fee upon proper indication by the counselor or concern team/person.

## Programme **Delivery**

*Live Online Sessions delivered Direct to Device (D2D)*

## Who's **this program is for?**

This program is designed to fulfill the upskilling requirements of undergraduate and graduating students specializing in BFSI, cybersecurity, and fin tech fields who already have a basic technical understanding of cyber security. It is especially beneficial for those aspiring to pursue job roles/positions such as, but not limited to:

- ✓ Ethical hacker
- ✓ Network Security Consultants
- ✓ Threat Hunters
- ✓ Risk Assessment Analysts
- ✓ Security Analysts
- ✓ Junior Penetration Testers
- ✓ Security Architects
- ✓ Graduate students & working professionals

# Pre-Requisites



**Basic Computer  
Fundamentals**



**Network  
Fundamentals**



**Network Devices  
Fundamentals**





# CORE TOPICS

- Module 1:-** Fundamentals and Essential Terminologies
- Module 2:-** Open Source Intelligence and Information Gathering
- Module 3:-** Windows and Linux Exploitation
- Module 4:-** Introduction to Malware Threats
- Module 5:-** Mobile Device Hacking
- Module 6:-** Wireless Hacking
- Module 7:-** Cryptography
- Module 8:-** Penetration Testing Concepts and Methodologies
- Module 9:-** Pre-Engagement Activities
- Module 10:-** Open Source Intelligence and Information Gathering
- Module 11:-** External Network Penetration Testing
- Module 12:-** Internal Network Penetration Testing Internal
- Module 13:-** Other Internal Penetration Testing Procedure
- Module 14:-** Automating Pen-testing
- Module 15:-** Perimeter Devices Penetration Testing
- Module 16:-** Clearing Tracks and Artifacts

# CORE TOPICS

- Module 17:-** Application Security Assessment/Penetration Testing
- Module 18:-** Fundamentals and Information Gathering
- Module 19:-** Content Discovery
- Module 20:-** Methodologies Analysis
- Module 21-** Non-Conventional Attacks & Business Logic Attacks
- Module 22:-** Fundamentals of Android Operating System
- Module 23:-** SSL Pinning & Types
- Module 24:-** Mobile Application Penetration Testing
- Module 25:-** Dyanamic Analysis
- Module 26:-** Reporting and Artifacts

## CYBER FORENSICS

- Module 27:-** Introduction to Computer Forensics
- Module 28:-** Investigation Process
- Module 29:-** Pre-requisite skills of Forensics
- Module 30:-** Data Acquisition and Techniques
- Module 31:-** Anti-Anti-Forensics Techniques
- Module 32:-** Windows Forensics

# CORE TOPICS

- Module 33:-** Linux and Mac Forensics
- Module 34:-** Network Forensics
- Module 35:-** Malware Forensics
- Module 36:-** Web Application attacks investigation
- Module 37:-** Forensics on Dark Web
- Module 38:-** Cloud Forensics
- Module 39:-** Email and Social Media Forensics
- Module 40:-** Mobile Forensics
- Module 41:-** Mobile Forensics

## Security Operation Center

- Module 42:-** Incidents, Events and Logging
- Module 43:-** Enhanced Incident Detection with Threat Intelligence
- Module 44:-** Internal Network Penetration Testing Internal
- Module 45:-** Security Information and Event Management
- Module 46:-** Enhanced Incident Detection with Threat Intelligence

## INCIDENT HANDLING

- Module 47:-** Incident Response
- Module 48:-** Incident Handling and Responsive Action

# CORE TOPICS

- Module 49:-** Incident handling and Response Process
- Module 50:-** First Action
- Module 51:-** Handling & Responding to Malware Incidents
- Module 52:-** Handling and Responding to Email Security Incidents
- Module 53:-** Handling and Responding to Network Security Incidents
- Module 54:-** Handling and Responding to Web Application Security
- Module 55:-** Handling and Responding to Cloud Security Incidents
- Module 56:-** Handling and Responding to Cloud Security Incidents
- Module 57:-** Endpoint Security Handling

## **Compliance Auditing - ISO 27001**

- Module 58:-** Standards, Principles and Definitions
- Module 59:-** ISMS history and Benefits
- Module 60:-** Information Risk Assessment and Treatment
- Module 61:-** ISO/IEC 27002 and the Control Objectives
- Module 62:-** ISMS Development Stages
- Module 63:-** Legal Compliance and ISMS
- Module 64:-** IT Security Techniques - IS Incident Management

# CORE TOPICS

- Module 65:-** Accreditation, Certification and Types of Audits
- Module 66:-** Audit Process & Planning
- Module 67:-** PLANNING: AUDIT PLAN
- Module 68:-** Checklists & Techniques to Follow on Audits
- Module 69:-** Conducting Audit - Raising Non-Conformities
- Module 70:-** Conducting Audits - Audit Reporting and Closing Meeting

## Course Fees











**₹ 1,75,000+ 18% GST**

✓ No cost EMI are Available



**Add the OSCP certification course for just ₹1,40,000 extra**

# Virtual Environment and Distributions

 Windows 11	 Windows Server 2019 Windows Server 2019	 Ubuntu	 Kali Linux	 Genymotion
 MOBEXLER FOR HICKERS   BY HICKERS	 NoxPlayer THE SIMPLER THE BETTER Nox Player	 Bluestacks	 Memu player	 Android Studio

## Tools

 OpenJDK	 NMAP	 VIRUSTOTAL	 SHODAN
 Nessus®	 Acunetix by Invicti	 HURRICANE ELECTRIC INTERNET SERVICES	 ExE
 Burp Suite	 cuckoo	 Metasploit	 OpenVAS Open Vulnerability Assessment Scanner
 Metasploit	 Atomic	 Arjun	 VeraCrypt
 MOBSF	 OBFUSCATOR	 OllyDbg	 Red Panda

# Learning Outcomes

- ✓ Mastering Network Penetration Testing
- ✓ Mastering Web Application Penetration Testing
- ✓ Mastering Ethical Hacking
- ✓ Mastering Endpoint Exploitation
- ✓ Mastering Malware Analysis Processes
- ✓ Mastering Industry demand Skills



# Career Support

<b>Personal Branding and Community Chaining</b>	Profile creation on professional networking platforms & focus on personal branding How to Connect with various Pentesting Communities of Twitter, Telegram and other Forums and Blogs.
<b>Business Communication</b>	Role and Importance of effective communication in professional world
<b>Industry Session -1</b>	Session by industry expert
<b>Job Search Strategy</b>	Resume building and review
<b>Interview Preparation</b>	Pre, In and post interview practices
<b>1:1 Personalised Coaching</b>	1:1 Personalised Coaching - 45 minutes each learner
<b>Industry Session -2</b>	Session by industry expert



# Certificate

Certificate ID:



**Electronics & ICT Academy**

**Indian Institute of Technology Guwahati**

*Supported by Ministry of Electronics and Information Technology (MeitY), Govt. of India*

## CERTIFICATE OF COMPLETION

This is to certify that Mr./Ms.

**Name**

has successfully completed the online

**“Post Graduate Certification Program in Cyber Security”**

organized by **Electronics & ICT Academy Indian Institute of Technology Guwahati**

held from --/--/---- to --/--/----

\_\_\_\_\_  
**Dr. Gaurav Trivedi**  
Principal Investigator  
Electronics & ICT Academy  
Indian Institute of Technology Guwahati

\_\_\_\_\_  
**Ms. Neha Singh**  
Director  
Securium Solutions Private Limited  
[Securium Academy]

*This is an online certification programme conducted jointly by E&ICT Academy, IIT Guwahati and Securium Academy towards upskilling.*

# Corporate Internship Opportunity



Partnering with Securium Solutions, a leading pioneer in cybersecurity services and consulting, and E&ICT Academy, IIT Guwahati and presents a remarkable opportunity for students to advance their careers in the cybersecurity field. Through this collaboration, students receive top-tier training accompanied by an esteemed E&ICT Academy, IIT Guwahati certificate, enhancing their professional credentials. This program not only equips participants with cutting-edge cybersecurity skills and knowledge but also provides a pathway to internships at Securium Solutions Private Limited. Such internships offer invaluable real-world experience, allowing students to apply their learning in practical settings, network with industry professionals, and gain insights into the latest industry practices. This combination of high-quality education, certification, and hands-on experience significantly boosts their career prospects, positioning them as highly skilled & competitive candidates in the rapidly evolving cybersecurity job market.

# Securium Solutions PVT. LTD. (Securium Academy)

[www.securiumsolutions.com](http://www.securiumsolutions.com) | [www.securiumacademy.com](http://www.securiumacademy.com)

## INDIA

Securium Solutions Pvt. Ltd.  
[Securium Academy]

B28, First Floor, Sector 1, Noida,  
Uttar Pradesh,  
India – 201301

Phone: 9080406859, 9704433355

## USA

Securium Solutions LLC

1968 S. COAST HWY  
2989 LAGUNA BEACH,  
CA 92651

United States

Phone: +13015437051