SECURIUM ACADEMY

Cyber Security

Master's Program

Table of Contents

About the Course

The Cyber Security Master's Program will equip you with the full range of skills needed to become an expert in this rapidly growing domain. You will learn comprehensive approaches to protecting your infrastructure, including securing data and information, running risk analysis and mitigation, architecting cloud-based security, achieving compliance and much more with this best-in-class program.

Key Features

150+ hours of instructor-led online classes

Exam voucher included for OSCP, CEHv12 & Sec+

100+ hours of e-learning content

Master's Certificate upon course completion

About Securium Academy

Securium Academy is a leader in digital skills training, focused on the emerging technologies that are transforming our world. Our Blended Learning approach drives learner engagement and is backed by the industry's highest completion rates. Partnering with professionals and companies, we identify their unique needs and provide outcome-centric solutions to help them achieve their professional goals.

Program Outcomes

- Install, configure and deploy public key infrastructure and network components while assessing and troubleshooting issues to support organizational security
- Master advanced hacking concepts to manage information security efficiently
- Design security architecture and framework for a secure IT operation
- Frame cloud data storage architectures and security strategies, and utilize them to analyze risks
- Protect data movement, perform disaster recovery, access CSP security and manage client databases
- Implement technical strategies, tools, and techniques to secure data and information for your organization
- Adhere to ethical security behaviour for risk analysis and mitigation
- Understand security in cloud computing architecture in depth
- Comprehend legal requirements, privacy issues and audit process methodologies within the cloud environment
- Focus on IT compliance and the integrity of enterprise systems to establish a more secure enterprise IT framework

Program Eligibility Criteria and Prerequisites

There are no prerequisites for this training program. Prior knowledge of any programming language is recommended but not mandatory.

Who Should Enroll in this Program?

This program caters to working professionals from a variety of industries and backgrounds; the diversity of our students adds richness to class discussions and interactions.

The following are the few professional profiles that are ideal students for this course:

- All levels of IT auditor/penetration tester
- Security consultants/managers
- IT directors/managers/consultants
- Security auditors/architects
- Security systems engineers
- Chief information security officers (CISOs)
- Chief compliance/privacy/risk officers
- Network specialists, analysts, managers, architects, consultants or administrators
- Technical support engineers
- Systems analysts or administrators

Learning Path

1. **Introduction to Cyber Security**
   2 hrs
2. **Certified Ethical Hacker**
   40 hrs
3. **Security+ SY0-701**
   40 hrs
4. **OSCP**
   72 hrs
5. **CISA**
   40 hrs
6. **CISM**
   40 hrs
7. **CISSP**
   48 hrs
8. **Masters Certificate**
   You will get individual certificates for each

Electives

- CySA+ or CSA

STEP 1 2 3 4 5 6 7

Introduction to Cyber Security

Securium Academy's Introduction to Cyber Security course for beginners is designed to give you a foundational look at today's cybersecurity landscape and provide you with the tools to evaluate and manage security protocols in information processing systems.

Key Learning Objectives

- Gain a comprehensive overview of cyber security principles and concepts
- Learn the challenges of designing a security program
- Develop and manage an information security program, perform business impact analysis, and carry out disaster recovery testing

Course Curriculum

- **Lesson 1 -** Course Introduction
- **Lesson 2 -** Cyber Security Fundamentals
- **Lesson 3 -** Enterprise Architecture and Components
- **Lesson 4 -** Information System Governance and Risk Assessment
- **Lesson 5 -** Incident Management

STEP 1 2 3 4 5 6 7

EC-COUNCIL CEHv12

The Securium Academy's CEH v12 Certified Ethical Hacker training (earlier CEH v11) and certification course provide hands-on classroom training to help you master the same techniques that hackers use to penetrate network systems and leverage them ethically to protect your own infrastructure. The extensive course focuses on 20 of the most popular security domains to provide a practical approach to essential security systems.

Key Learning Objectives

After completing this course you will be able to:

- Ace the CEH exams
- Learn to assess computer system security by using penetration testing techniques
- Scan, test and hack secure systems and applications, and gain hands-on experience with sniffing, phishing and exploitation tactics

Course Curriculum

- **Module 01:** Introduction to Ethical Hacking - Overview of information security, threats, attack vectors, ethical hacking concepts, information security controls, penetration testing concepts, and information security laws and standards are covered in this module
- **Module 02:** Footprinting and Reconnaissance - These modules cover concepts and types of footprinting, footprinting through search engines, web services, and social networking sites, footprinting tools, countermeasures, and footprinting pen testing

- **Module 03:** Scanning Networks - Learn about network scanning concepts, tools and techniques, network diagrams, and scanning pen testing

- **Module 04:** Enumeration - Enumeration concepts, types, techniques, and pen testing are covered in this module

- **Module 05:** Vulnerability Analysis - Overview of vulnerability assessment concepts, solutions, scoring systems, tools, and reports are explained in this module

- **Module 06:** System Hacking - Learn how to crack passwords, hide files, cover tracks, any many more

- **Module 07:** Malware Threats - This module gets you familiar with malware concepts, trojan concepts, malware analysis, countermeasures, malware penetration testing

- **Module 08:** Sniffing - Sniffing concepts, tools, and techniques are explained in this module

- **Module 09:** Social Engineering - Comprehend social engineering concepts, techniques, countermeasures, and pen testing

- **Module 10:** Denial-of-service - Dos/DDoS concepts, techniques, tools, case studies, and penetration testing are covered in this module

- **Module 11:** Session Hijacking - Know what is session hijacking and its types, tools, countermeasures, and session hijacking penetration testing

- **Module 12:** Evading IDS, Firewalls, and Honeypots - Learn about firewalls and honeypots and how to detect and evade them

- **Module 13:** Hacking Web Servers - This module focuses on web server concepts, attacks, methodologies, tools, countermeasures, and penetration testing

- **Module 14:** Hacking Web Applications - Web app concepts, tools, methodologies, countermeasures, and penetration testing are covered in this module

- **Module 15:** SQL Injection - Get familiar with SQL Injection concepts, types, tools, methodologies, countermeasures, and penetration testing

- **Module 16:** Hacking Wireless Networks - Wireless concepts, threats, methodologies are covered in this module

- **Module 17:** Hacking Mobile Platforms - Learn how to hack android IOS, Mobile spyware, device management, security tools, and many more in this module

- **Module 18:** IoT Hacking - This module covers IoT Hacking concepts, attacks, methodologies, tools, countermeasures, and penetration testing

- **Module 19:** Cloud Computing - Concepts, attacks, methodologies, tools, countermeasures, and penetration testing of cloud computing are covered in this module

- **Module 20:** Cryptography - This module will teach you about cryptography concepts, encryption algorithms, tools, PKI, types of encryption, cryptanalysis, and countermeasures

STEP 1 2 3 4 5 6 7

CompTIA Security+ SY0-701

The CompTIA Security+ course will enable learners to gain knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; operate with an awareness of applicable policies, laws, and regulations. Upon successfully validating their skills by passing the certification exam learners will be able to perform these tasks to support the principles of confidentiality, integrity, and availability. CompTIA Security+ meets the ISO 17024 standard and is approved by the U.S.

Key Learning Objectives

- Comprehend risk identification and mitigation
- Provide operational, information, application and infrastructure level security
- Secure the network to maintain the availability, integrity and confidentiality of critical information
- Operate within a set of rules, policies and regulations wherever applicable

Course Curriculum

- **Lesson 1 -** Lesson 01 - Learn about networking, firewalls, LAN security, IDS, NAC, IPSec
- Lesson 02 - Understand the principles of security, risk management, data classification, disaster recovery, and forensics
- Lesson 03 - Comprehend cyber attacks, DNS security, social engineering fundamentals, buffer overflows, security testing tools usage, honeypots, vulnerability and pen testing

- Lesson 04 - Learn how to handle bugs, secure storage platforms and the power grid, how to hack IOT
- Lesson 05 - Get familiar with access controls, Kerberos, identity federation, and id governance
- Lesson 06 - Encryption, advanced cryptography, crypto algorithm, PKI, etc are covered in this lesson

Offensive Security - OSCP/PEN200

OSCP (Offensive Security Certified Professional) is a highly regarded certification in information security that validates a candidate's practical skills in penetration testing and ethical hacking. To prepare for the certification, candidates must complete the "Penetration Testing with Kali Linux" course offered by Offensive Security, which covers topics such as reconnaissance, scanning, exploitation, post-exploitation, and report writing. The OSCP exam is a 24-hour practical exam that requires candidates to demonstrate their skills in identifying and exploiting vulnerabilities in a simulated environment. OSCP certification is challenging but highly respected in the information security industry.

Key Learning Objectives

- Penetration Testing Methodology
- Network Penetration Testing
- Web Application Penetration Testing
- Buffer Overflow Exploitation
- Reporting and Documentation
- Access to the latest retired OSCP exam machines - new!
- Learn the "Try Harder" method and mindset
- Earn the industry-leading OSCP certification
- Introduction to the latest hacking tools and techniques
- Training from the experts behind Kali Linux

Course Curriculum

- MODULE 01: Penetration Testing: What You Should Know
- MODULE 02: Getting Comfortable with Kali Linux
- MODULE 03: Command Line Fun
- MODULE 04: Practical Tools
- MODULE 05: Bash Scripting
- MODULE 06: Passive Information Gathering
- MODULE 07: Active Information Gathering
- MODULE 08: Vulnerability Scanning
- MODULE 09: Web Application Attacks
- MODULE 10: Introduction to Buffer Overflows
- MODULE 11: Windows Buffer Overflows
- MODULE 12: Linux Buffer Overflows
- MODULE 13: Client-Side Attacks
- MODULE 14: Locating Public Exploits
- MODULE 15: Fixing Exploits
- MODULE 16: File Transfers
- MODULE 17: Antivirus Evasion
- MODULE 18: Privilege Escalation
- MODULE 19: Password Attacks
- MODULE 20: Port Redirection and Tunneling
- MODULE 21: Active Directory Attacks
- MODULE 22: The Metasploit Framework
- MODULE 23: PowerShell Empire
- MODULE 24: Assembling the Pieces: Penetration Test Breakdown
- MODULE 25: Trying Harder: The Labs

CISA - Key Learning Objectives

CISA certification is foundational to a successful IT career. If you are an entry-level to mid-career professional, CISA Certification can showcase your expertise and assert your ability to apply a risk-based approach to planning, executing, and reporting on audit engagements.Gain instant credibility in your interactions with internal stakeholders, regulators, external auditors, and customer

Key Learning Objectives

- Information System Auditing Process
- Governance and Management of IT
- Information Systems Acquisition, Development, and Implementation
- Information Systems Operations and Business Resilience
- Protection of Information Assets

Course Curriculum

- Module 01 - Information System Auditing Process
- Module 02 - Governance and Management of IT
- Module 03 - Information Systems Acquisition, Development, and Implementation
- Module 04 - Information Systems Operations and BusinessResilience
- Module 05 - Protection of Information Assets

CISM - Key Learning Objectives

The CISM certification, which is focused on management, promotes worldwide security practices and acknowledges the professional who manages, designs, oversees, and assesses an organization's information security. The CISM certification is the worldwide recognized benchmark of excellence in this field, and the demand for skilled information security management experts is on the rise.

Key Learning Objectives

- Information Security Governance
- Information Risk Management and Compliance
- Information Security Program Development and Management
- Information Security Incident Management

Course Curriculum

- Domain 1: Information Secuirty Governance
- Domain 2: Information Security Risk Management
- Domain 3: Information Security Program
- Domain 4: Incident Management

STEP 1 2 3 4 5 6 7

CISSP

Securium Academy's CISSP certification training is aligned with the (ISC)^2 CBK 2018 requirements. The course trains you in the industry's latest best practices, which will help you pass the exam in the first attempt. The certification helps you develop expertise in defining the architecture and in designing, building, and maintaining a secure business environment for your organization using globally approved Information Security standards.

Key Learning Objectives

- Be able to define the architecture, design and management of the security of your organization.
- Acquire the relevant knowledge and skills required to pass the CISSP certification exam.
- Earn the requisite 30 CPEs required to take up the CISSP certification exam.
- Develop working knowledge in the 8 domains prescribed by the CISSP Common Book of Knowledge, 2018.

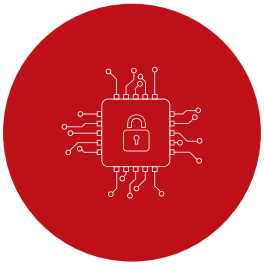
Course Curriculum

- **Lesson 00:** Introduction to CISSP - Overview of CISSP, CISSP Exams, ISC2 is covered in this lesson
- **Lesson 01:** Security and Risk Management - Information security management, risk analysis, legal systems, IP laws, BCA, CIA, etc are covered in this lesson
- **Lesson 02:** Asset Security - Learn how to classify information, protect privacy, maintain ownership, establish handling requirements

- **Lesson 03:** Security Engineering - Understand security engineering processes using secure design principles, Architecture Frameworks, Security Models Evaluation Criteria, Distributed Systems, and many more
- **Lesson 04:** Communications and Network Security - Learn how to secure network architecture, design, components, and communication channels
- **Lesson 05:** Identity and Access Management - Implement and manage authorization mechanisms to prevent or mitigate access control attacks
- **Lesson 06:** Security Assessment and Testing - Learn how to design and validate assessment and test strategies
- **Lesson 07:** Security Operations - Understand and support requirements for investigations by implementing resource protection techniques and incident response
- **Lesson 08:** Software Development Security - Comprehend the system life cycle and system development in this lesson

Elective Course

CompTIA CySA+ Network



The CompTIA CySA+ (Cybersecurity Analyst+) (CS0-003) certification training program focuses on cybersecurity's technical and hands-on aspects, encompassing cyber threats, secure network architecture, risk management, log analysis, configuration assessments, and more. Upon successful completion, individuals are equipped with the necessary knowledge and skills to effectively identify, analyze, and interpret indicators of malicious activity. They gain a comprehensive understanding of threat intelligence and management, enabling them to respond to various attacks and vulnerabilities proactively. Additionally, candidates learn incident response methodologies to handle security incidents and mitigate their impact efficiently.

EC-COUNCIL CSA

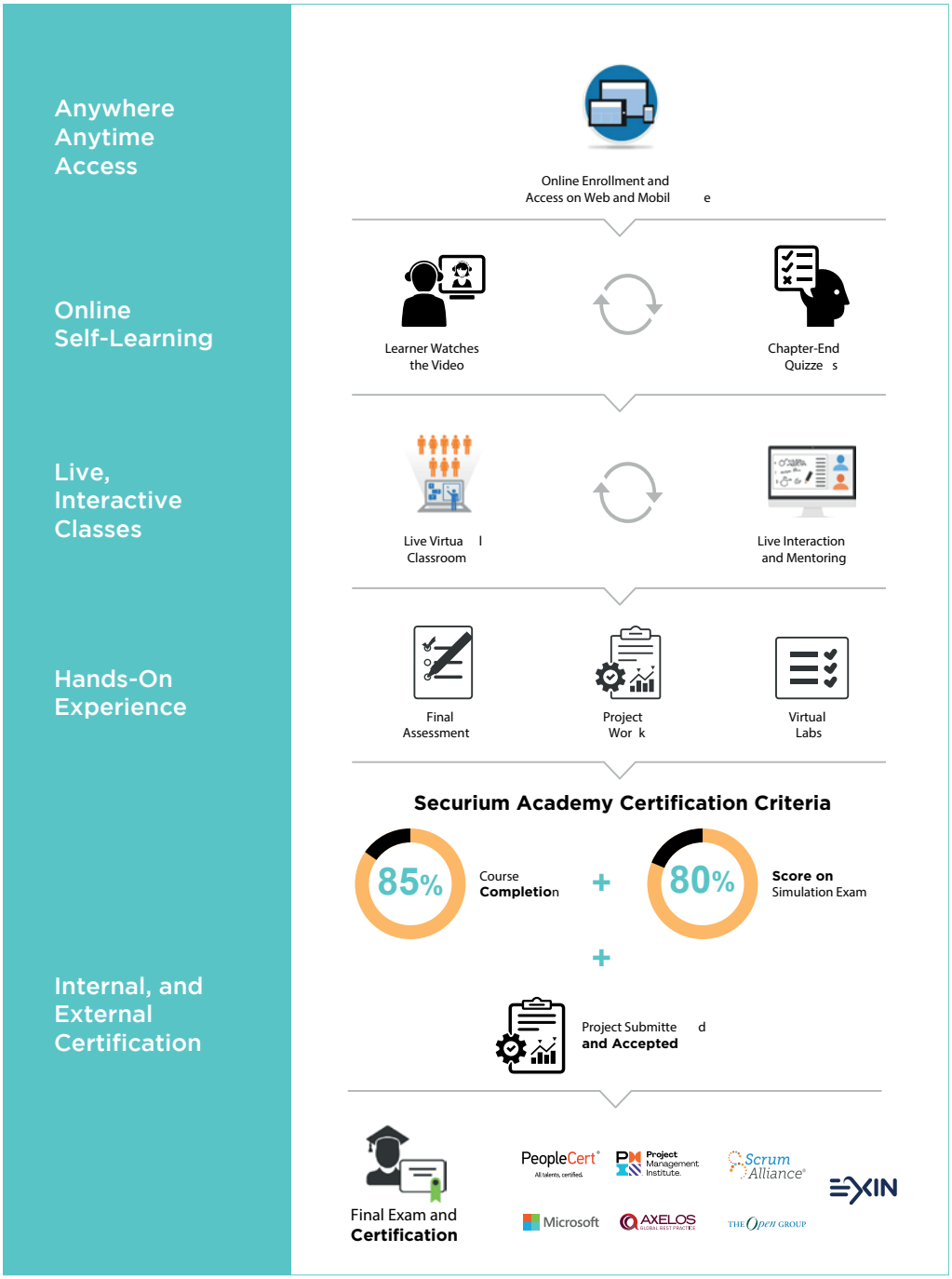
EC-Council Certified SOC Analyst Training Program will help you to master over trending and in-demand technical skills like Knowledge of SOC processes, procedures of these processes, technologies, and workflows. basic understanding and detailed knowledge of security threats, attacks, vulnerabilities, attacker's behaviours, cyber kill chain, etc. Through this SOC Analyst Certification Training our expert trainers offer in-depth knowledge with enhanced level capabilities for dynamic contribution to a SOC team. CSA Training Course has been especially designed to help you learn :The basics of SOC operations, log management and correlation, SIEM deployment, advanced incident detection, and incident response

This SOC Analyst course will also help you to improve your knowledge regarding performance of enhanced threat detection using the predictive capabilities of Threat Intelligence.

Certificate

Upon completion of this Master's Program, you will receive the certificates from Securium Academy in the Cyber Security courses in the learning path. These certificates will testify to your skills as an expert in Cyber Security. Upon completion, you will also receive an industry-recognized Master's Certificate from Securium Academy.

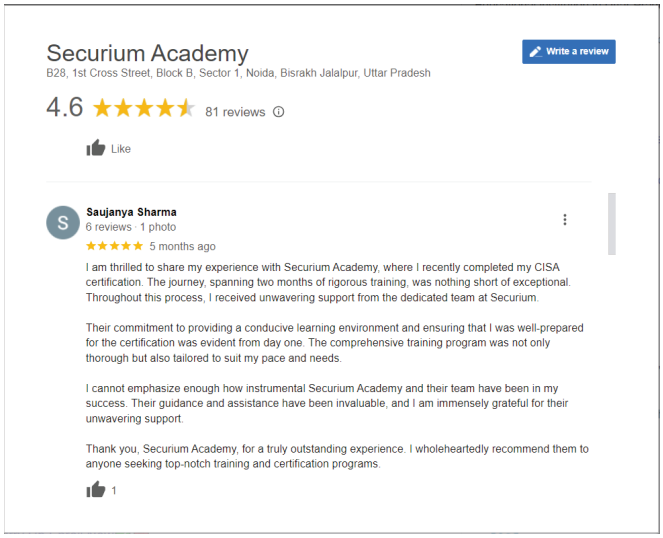
Classroom-Level Immersion: Delivered Digitally



Customer Reviews

Riya Ahuja

The instructor SAM provided excellent CEHv10 online classroom training using practical exercises and EC-Council content, as well as sharing his priceless personal knowledge and wisdom.



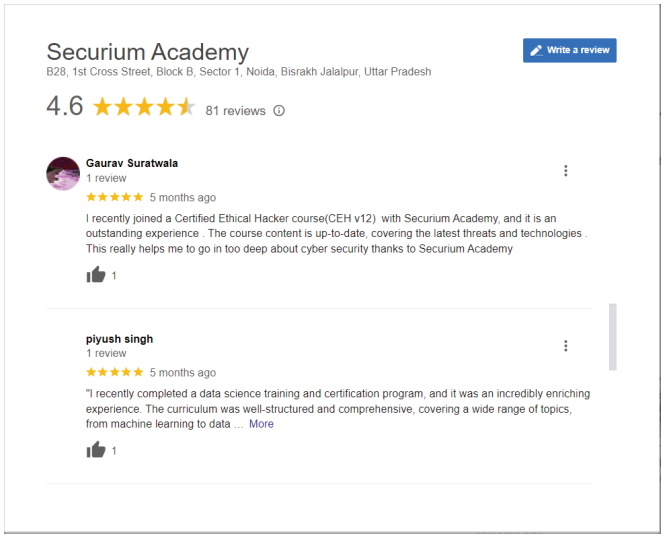
Securium Academy
B28, 1st Cross Street, Block B, Sector 1, Noida, Bisrakh Jalalpur, Uttar Pradesh
Write a review
4.6 ★★★★½ 81 reviews
Like

Saujanya Sharma
6 reviews · 1 photo
★★★★★ 5 months ago
I am thrilled to share my experience with Securium Academy, where I recently completed my CISA certification. The journey, spanning two months of rigorous training, was nothing short of exceptional. Throughout this process, I received unwavering support from the dedicated team at Securium.

Their commitment to providing a conducive learning environment and ensuring that I was well-prepared for the certification was evident from day one. The comprehensive training program was not only thorough but also tailored to suit my pace and needs.

I cannot emphasize enough how instrumental Securium Academy and their team have been in my success. Their guidance and assistance have been invaluable, and I am immensely grateful for their unwavering support.

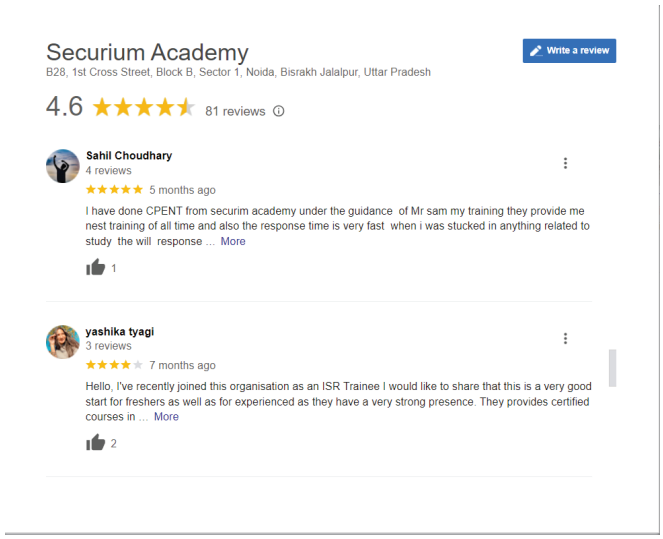
Thank you, Securium Academy, for a truly outstanding experience. I wholeheartedly recommend them to anyone seeking top-notch training and certification programs.
1



Securium Academy
B28, 1st Cross Street, Block B, Sector 1, Noida, Bisrakh Jalalpur, Uttar Pradesh
Write a review
4.6 ★★★★½ 81 reviews

Gaurav Suratwala
1 review
★★★★★ 5 months ago
I recently joined a Certified Ethical Hacker course(CEH v12) with Securium Academy, and it is an outstanding experience . The course content is up-to-date, covering the latest threats and technologies . This really helps me to go in too deep about cyber security thanks to Securium Academy
1

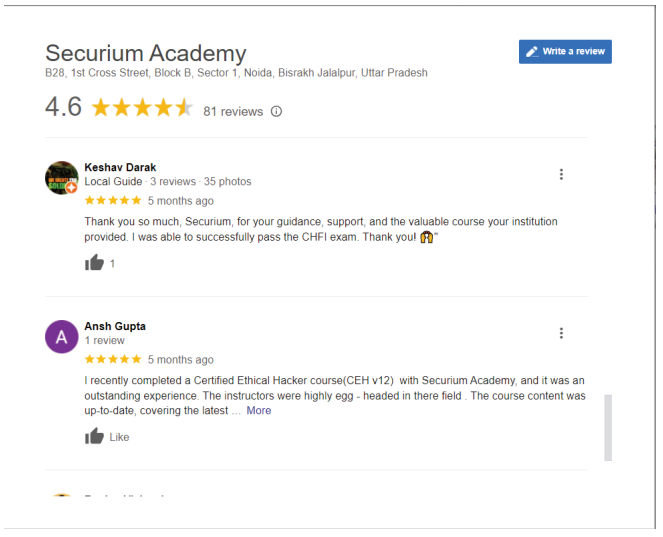
piyush singh
1 review
★★★★★ 5 months ago
"I recently completed a data science training and certification program, and it was an incredibly enriching experience. The curriculum was well-structured and comprehensive, covering a wide range of topics, from machine learning to data … More
1



Securium Academy
B28, 1st Cross Street, Block B, Sector 1, Noida, Bisrakh Jalalpur, Uttar Pradesh
Write a review
4.6 ★★★★½ 81 reviews

Sahil Choudhary
4 reviews
★★★★★ 5 months ago
I have done CPENT from securim academy under the guidance of Mr sam my training they provide me nest training of all time and also the response time is very fast when i was stucked in anything related to study the will response … More
1

yashika tyagi
3 reviews
★★★★☆ 7 months ago
Hello, I've recently joined this organisation as an ISR Trainee I would like to share that this is a very good start for freshers as well as for experienced as they have a very strong presence. They provides certified courses in … More
2



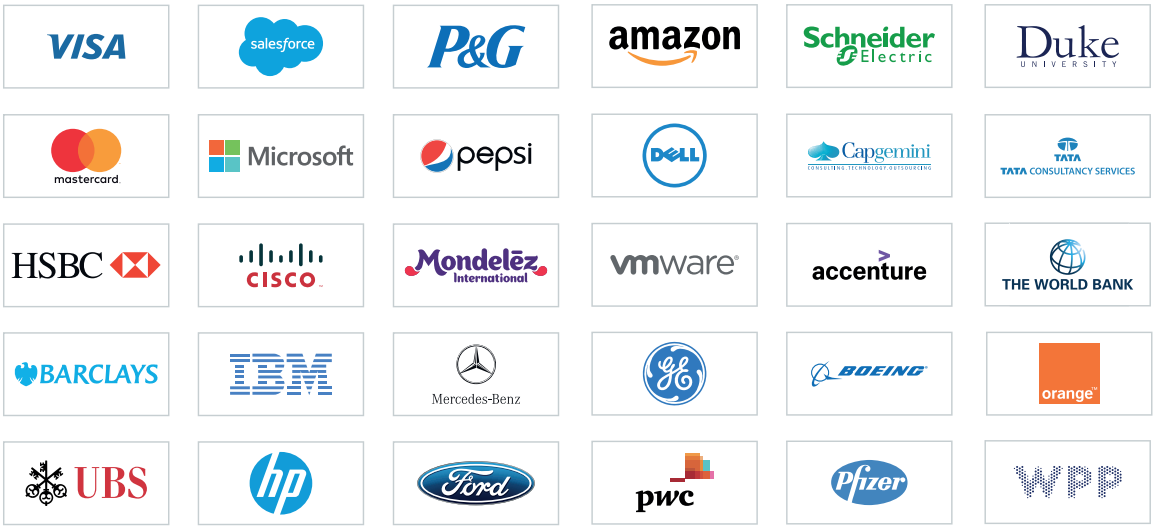
Securium Academy
B28, 1st Cross Street, Block B, Sector 1, Noida, Bisrakh Jalalpur, Uttar Pradesh
Write a review
4.6 ★★★★½ 81 reviews

Keshav Darak
Local Guide · 3 reviews · 35 photos
★★★★★ 5 months ago
Thank you so much, Securium, for your guidance, support, and the valuable course your institution provided. I was able to successfully pass the CHFI exam. Thank you!
1

Ansh Gupta
1 review
★★★★★ 5 months ago
I recently completed a Certified Ethical Hacker course(CEH v12) with Securium Academy, and it was an outstanding experience. The instructors were highly egg - headed in there field . The course content was up-to-date, covering the latest … More
Like

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

Securium Solutions Pvt. Ltd.

B28, 1st Cross Street,
Block B, Sector 1, Noida,
Uttar Pradesh 201301

DUBAI

Securium Solutions Pvt. Ltd.

Downtown Office 202,
Saaha Office, C- Soukm Al
Bahar Bridge, Dubai, Po
Box : 282615

www.securiumacademy.com