ITA Associates

Cyber Security

Master's Program

Powered by simplilearn

Content Aligned to CompTIA. CISSP. EC-Council

Table of Content

About the Program

This Cybersecurity Expert Program equips you with essential skills and knowledge to excel in high-demand cybersecurity roles. It prepares you for certifications like CEH , CompTIA Security, and CISSP . The program includes hands-on labs, live classes, and real-world simulations to ensure mastery of critical skills, such as ethical hacking, risk management, cloud security, and network protection.

Excel in your learning with live, expert-led sessions and hands-on practice in a simulated environment. Apply acquired skills to real-world challenges through Capstone projects and advanced labs, focusing on penetration testing, AI-powered threat detection, cloud security, and more. Gain practical experience in designing secure IT infrastructure, mastering cybersecurity principles, and responding to advanced cyber threats.

Upon completion, you'll gain access to Simplilearn's Job Assistance services, including career mentoring, resume building, and interview preparation.

Key Features of the Program

Course curriculum aligned with the latest CEH , CompTIA Security, and the CISSP certification exams

Get a CEH exam voucher with 6 months of complimentary iLabs access for hands-on practice

Master 30+ in-demand tools and skills, including ethical hacking, network security, and risk management strategies

Take simulation tests focused on exam preparation to ensure you're fully equipped.

Experience 8X more interaction in live online classes led by accredited cybersecurity experts

Get Learner Success Manager to support you throughout your certification journey

Enjoy lifetime access to self-paced videos and class recordings for continuous learning

Simplilearn's JobAssist helps you get noticed by top hiring companies in the cybersecurity field (India Only)

Partnerships and Certifications Alignment

This Cybersecurity Expert Program is aligned with the curriculum of leading industry certifications, including CEH v13 AI, CompTIA Security+ 701, and CISSP (2024). We are partnered with EC-Council to deliver this program.

About Simplilearn

Founded in 2010 and based in San Francisco, California, and Bangalore, India, Simplilearn, a Blackstone portfolio company, is a global leader in digital upskilling, enabling learners across the globe offering access to world-class training to individuals and businesses worldwide. Simplilearn offers 1,500+ live classes each month across 150+ countries, impacting over 8 million learners globally. The programs are designed and delivered with world-renowned universities, top corporations, and leading industry bodies via live online classes featuring top industry practitioners, sought-after trainers, and global leaders. From college students and early career professionals to managers, executives, small businesses, and big corporations, Simplilearn's role-based, skill-focused, industry-recognized, and globally relevant training programs are ideal upskilling solutions for diverse career or business goals.

Eligibility Criteria

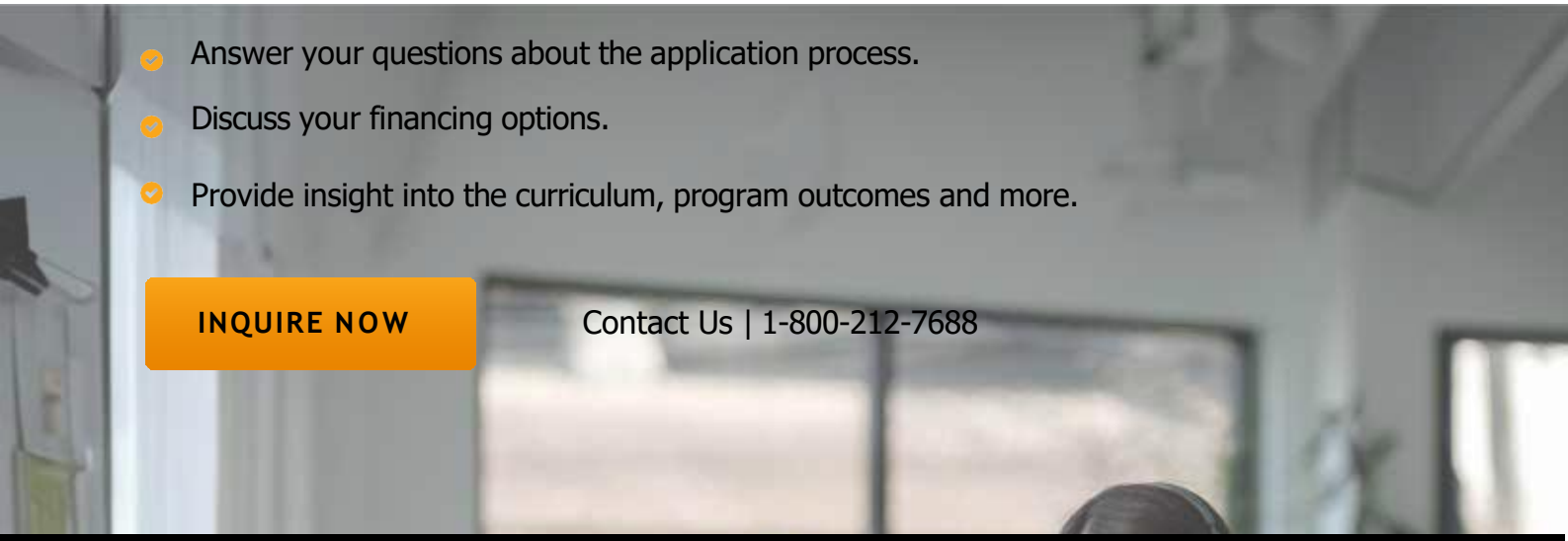
For admission into this program, candidates:

- Should be at least 18 years old and have a high school diploma or equivalent
- Basic understanding of IT and security concepts is recommended but not required
- Are not required to have prior professional experience

Talk to an Admissions Counselor

Our team of dedicated admissions counselors is prepared to address your questions or concerns about the Cloud Computing Bootcamp.

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

76% of Companies Targeted

Organizations were targeted by ransomware attacks globally, a trend expected to grow.

Source: ISACA

66% Unprepared for AI Attacks

66% of organizations are not equipped to handle AI-powered cyber threats effectively.

Source: EC-Council

USD 500 billion Market

The global cybersecurity market is projected to reach USD 479 billion by 2030, with a high CAGR.

Source: Grand View Research

Cybersecurity Career Outlook

Due to the high demand for Cybersecurity professionals, salaries in this field often reflect the reality of the market. The company's size, geographical location, and industry can significantly influence compensation levels. Taking these variables into consideration, we have compiled an estimate of what you can expect to earn in the following roles:

Ethical Hacker

Ethical hackers simulate cyberattacks on an organization's systems to identify vulnerabilities and weaknesses. They use the same tactics, techniques, and procedures as malicious hackers but with the goal of improving security measures.

Average Salary Range -
$88,000 - $132,000

Penetration Tester

A penetration tester conducts authorized simulated attacks on computer systems, networks, and web applications to discover potential security breaches. They help organizations enhance their defenses by providing actionable insights based on their findings.

Average Salary Range -
$92,000 - $136,000

Information Security Analyst

An information security analyst is responsible for protecting an organization's computer systems and networks. They implement security measures, monitor for potential breaches, and develop response protocols to address incidents.

Average Salary Range -
$80,000 - $120,000

Security Administrator

A security administrator manages an organization’s security systems, ensuring that they are up- to- date and functioning correctly. They are responsible for enforcing security policies and maintaining firewalls, antivirus software, and monitoring tools.

Average Salary Range -
$85,000 - $125,000

Security Consultant

A security consultant provides expert advice on securing an organization’s systems. They assess current security measures, identify vulnerabilities, recommend improvements, and help implement new security protocols.

Average Salary Range -
$100,000 - $155,000

Information Security Manager

An information security manager oversees an organization's security strategy, managing security teams, and ensuring that policies and procedures align with business goals. They handle incident responses, risk assessments, and compliance with security regulations.

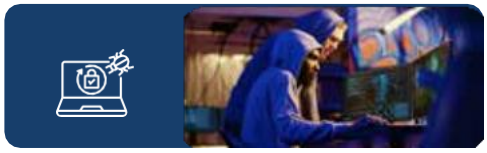
Average Salary Range -
$120,000 - $175,000

Eligible Job Roles after the completion of the program

This program is designed to train professionals who will be responsible for cloud computing in their respective organizations and is recommended for individuals pursuing positions including, but not limited to:

Ethical Hacker

Penetration Tester



Security Consultant

Information Security Manager

Security Architect

IT Security Specialist

Cybersecurity Analyst

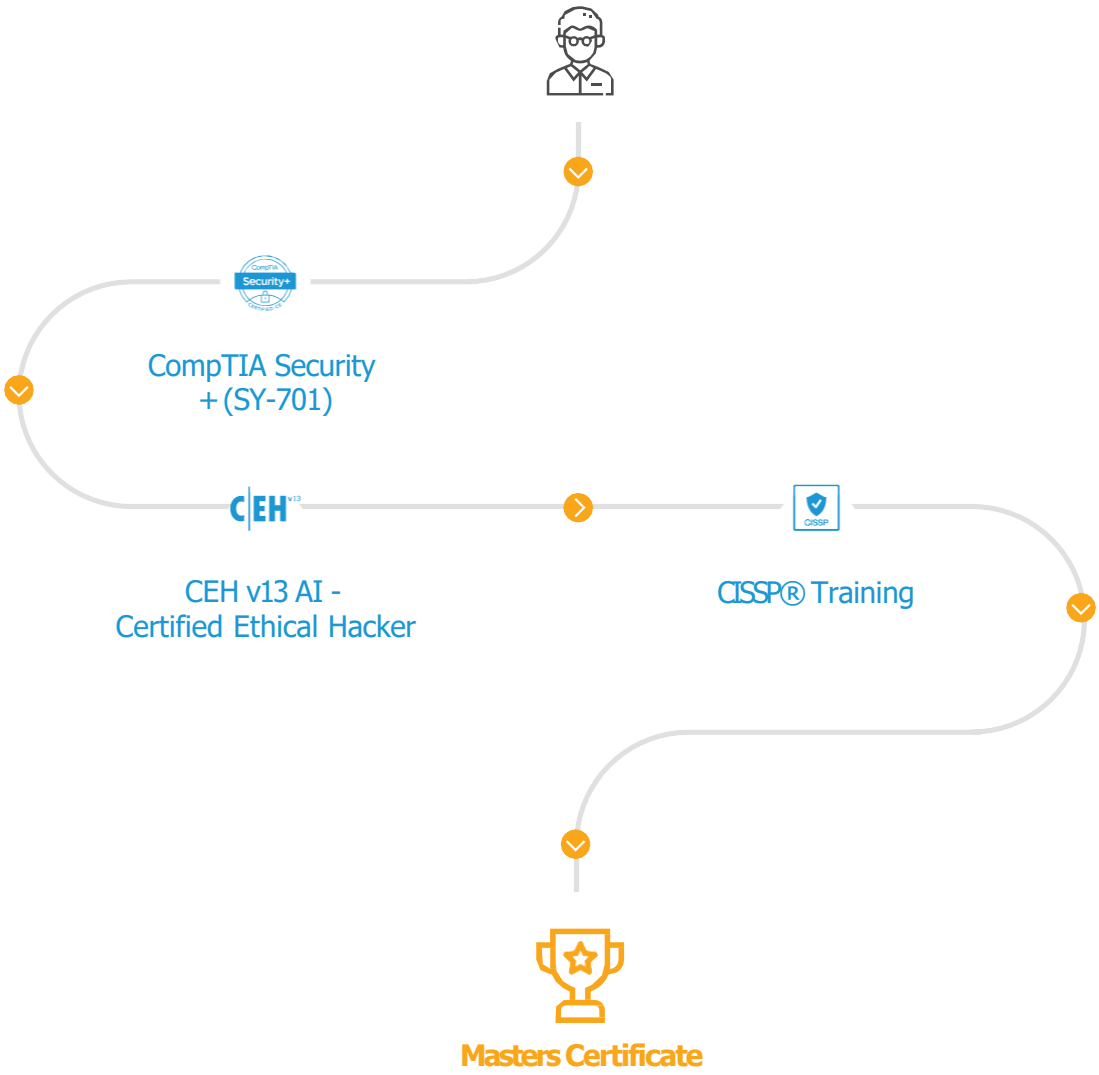
Network Security Engineer

Security Operations Center (SOC) Analyst

Chief Information Security Officer (CISO)

Learning Path

Introduction to Cybersecurity



Electives:

- Step 1- CCSP (Certified Cloud Security Professional)
- Step 2 - CompTIA Network+
- Step 3 - CISM (Certified Information Security Manager)

STEP 1

Course 1 - CompTIA Security + (SY-701)

This course equips learners with the essential skills to securely install and configure systems across applications, networks, and devices. It covers threat analysis, mitigation techniques, risk management, and compliance with industry standards. Successfully passing the certification exam confirms your ability to uphold confidentiality, integrity, and availability within an organization. CompTIA Security+ is ISO 17024 certified and recognized by the U.S. Department of Defense.

Key Learning Objectives

- Grasp the fundamentals of security, risk management, and applying security controls.
- Learn how to detect and mitigate different cyber threats and vulnerabilities.
- Understand security policies, laws, and regulations, and ensure organizational compliance.

Course Curriculum

- Lesson 01 – Explore networking basics and core security technologies, focusing on secure network architecture and devices.
- Lesson 02 – Understand key security concepts, risk management, and data protection, emphasizing compliance and governance.
- Lesson 03 – Study cyber attack techniques and learn defensive security testing methods like vulnerability scanning and penetration testing.
- Lesson 04 – Learn to manage vulnerabilities and safeguard critical infrastructure, including cloud, mobile, and IoT security.
- Lesson 05 – Examine cybersecurity policies, laws, and regulations, with a focus on data privacy and regulatory compliance.

STEP 2

Course 2 - CEH v13 AI - Certified Ethical Hacker

This Simplilearn course provides hands-on training in AI-powered ethical hacking techniques to secure networks and systems. Covering 20 essential security domains, it equips you with advanced, AI-driven methods to tackle modern cyber threats

Key Learning Objectives

- Master AI-driven skills to excel in the CEH v13 practical exam.
- Leverage AI for advanced penetration testing and system security assessments.
- Gain practical experience using AI-enhanced tools for scanning, hacking, and exploiting systems.

Course Curriculum

- Lesson 1: Introduction to Ethical Hacking
  Learn fundamentals of information security, ethical hacking concepts, laws, and procedures.
- Lesson 2: Footprinting and Reconnaissance
  Explore tools and techniques for footprinting and reconnaissance in pre-attack stages.
- Lesson 3: Scanning Networks
  Study various network scanning methods to identify vulnerabilities and countermeasures.
- Lesson 4: Enumeration
  Learn enumeration techniques like BGP and NFS exploits, plus their countermeasures.
- Lesson 5: Vulnerability Analysis
  Master methods for identifying security loopholes using vulnerability assessments.
- Lesson 6: System Hacking Methodologies
  Explore techniques like steganography, system hacking, and covering tracks.
- Lesson 7: Malware Threats and Analysis
  Understand malware types, analysis processes, and mitigation strategies.
- Lesson 8: Sniffing
  Learn packet sniffing techniques and defense strategies against sniffing attacks.
- Lesson 8: Sniffing
  Learn packet sniffing techniques and defense strategies against sniffing attacks.

- Lesson 9: Social Engineering
  Study social engineering tactics, theft attempts, and human vulnerability countermeasures.
- Lesson 10: Denial of Service (DoS/DDoS)
  Understand DoS and DDoS attack methods, tools, and protection strategies.
- Lesson 11: Session Hijacking
  Explore session hijacking techniques and cryptographic weaknesses with defenses.
- Lesson 12: Evading IDS, Firewalls, and Honeypots
  Learn how to evade security measures like IDS, firewalls, and honeypots, with countermeasures.
- Lesson 13: Hacking Web Servers
  Master auditing vulnerabilities in web servers and applying countermeasures.
- Lesson 14: Hacking Web Applications
  Learn about web application vulnerabilities and auditing methodologies.
- Lesson 15: SQL Injection
  Understand SQL injection attacks, evasion techniques, and their countermeasures.
- Lesson 16: Hacking Wireless Networks
  Study wireless encryption, hacking methodologies, tools, and defense strategies.
- Lesson 17: Hacking Mobile Platforms
  Learn about mobile platform attack vectors, hacking techniques, and security tools.
- Lesson 18: IoT Hacking
  Understand IoT/OT hacking methodologies, tools, and protection strategies.
- Lesson 19: Cloud Computing
  Study cloud threats, attacks, and security tools for cloud infrastructures.
- Lesson 20: Cryptography
  Learn cryptography algorithms, encryption techniques, and cryptanalysis tools.

STEP 3

Course 3 - CISSP® Training

This course aligns with the (ISC)² CISSP 2024 Common Body of Knowledge (CBK). It is designed to train you in the latest industry best practices and help you pass the CISSP exam on your first attempt. This certification provides expertise in designing, building, and maintaining secure business environments based on global standards.

Key Learning Objectives

- Master advanced cybersecurity practices to define, design, and manage your organization's security architecture.
- Gain the skills needed to pass the CISSP 2024 certification exam successfully.
- Build practical expertise across the 8 CISSP domains, including Security and Risk Management, Security Architecture and Engineering, and more.

Course Curriculum

- Lesson 00: Introduction to CISSP
  Overview of CISSP certification, exam structure, and (ISC)².
- Lesson 01: Security and Risk Management
  Covers risk management, legal systems, and the CIA triad.
- Lesson 02: Asset Security
  Focuses on data classification, privacy, and secure handling of information.
- Lesson 03: Security Architecture and Engineering
  Explores secure design principles, cryptography, and distributed systems.
- Lesson 04: Communications and Network Security
  Learn to secure networks, design architecture, and protect communication channels.
- Lesson 05: Identity and Access Management (IAM)
  Understand access control, authorization, and attack mitigation strategies.
- Lesson 06: Security Assessment and Testing
  Design and execute security testing and vulnerability assessments.
- Lesson 07: Security Operations
  Covers incident response, resource protection, and disaster recovery.

- Lesson 08: Software Development Security
  Learn secure SDLC practices and address software vulnerabilities.

Electives:

CCSP (Certified Cloud Security Professional)

Get introduced to cloud security fundamentals and learn to implement security controls across platforms. Master essential tools and apply cloud security concepts with a focus on compliance, risk, and governance.

CompTIA Network+

Build a strong foundation in networking fundamentals, learning how to configure, manage, and troubleshoot networks. Apply networking concepts to ensure security, reliability, and performance in real-world environments.

CISM (Certified Information Security Manager)

Gain expertise in information security management with a focus on governance, risk, and compliance. Learn to design and manage security programs aligned with business goals to protect sensitive data and systems.

Program Outcomes

By the end of this program, you will be able to:

- Install, configure, and deploy Public Key Infrastructure (PKI) and network components while assessing and troubleshooting issues to support organizational security needs.
- Master advanced ethical hacking techniques to effectively manage and enhance information security practices within an organization.
- Design and implement security architecture frameworks for securing IT operations across enterprise environments.
- Develop and secure cloud data storage architectures and security strategies, and utilize them to assess and mitigate associated risks.
- Protect data movement, implement disaster recovery plans, manage cloud service provider (CSP) security, and oversee client database security.
- Implement technical strategies, tools, and techniques to safeguard organizational data and sensitive information.
- Understand legal requirements, privacy concerns, and audit methodologies within the cloud environment to maintain compliance and security.
- Gain in-depth knowledge of security in cloud computing architectures and apply it to ensure the secure deployment of cloud environments.
- Adhere to ethical security practices to conduct risk analysis and mitigation efficiently.
- Focus on IT compliance and system integrity, ensuring a secure and resilient enterprise IT framework.

Skills Covered

- Ethical Hacking
- Malware Analysis
- Penetration Testing Methodologies
- Advanced Hacking Concepts
- Trojans, Backdoors, and Countermeasures
- Network Security
- Identity and Access Management
- Cryptography
- Incident Response and Management
- Data Loss Prevention (DLP)
- Security and Risk Management
- Software Development Security
- Security Assessment and Testing
- Compliance Frameworks
- Security Architecture

Tools Covered:

Nmap

Metasploit

Wireshark

Burp Suite

OpenVAS

Nessus

Kali Linux

Snort

Splunk

Hydra

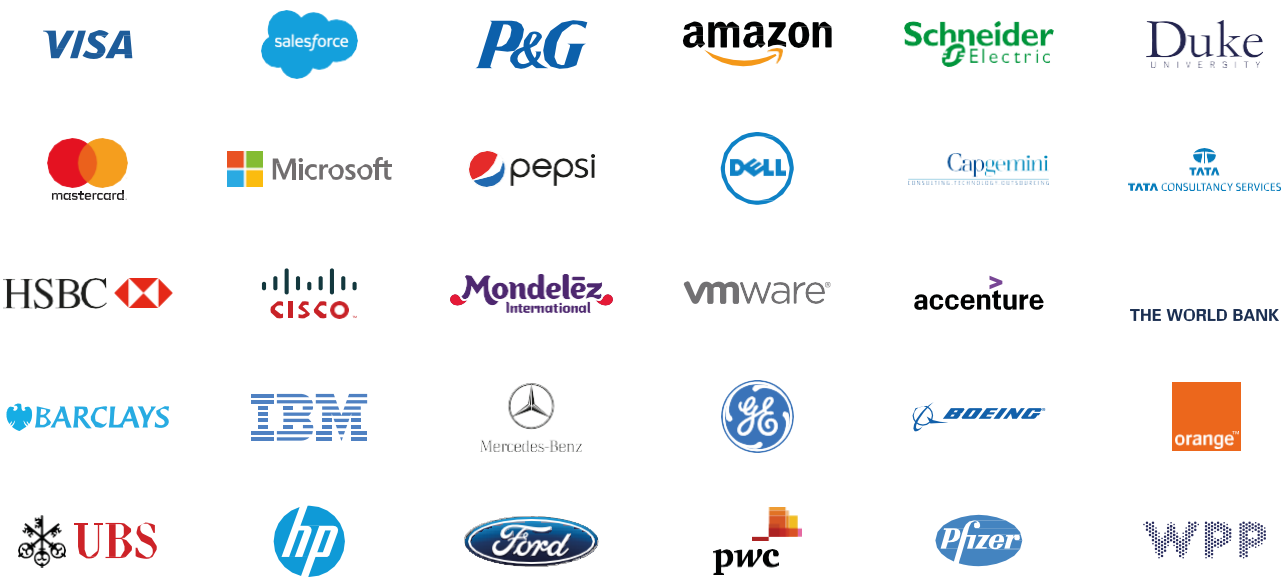
ShelGPT

Certificate

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

United Kingdom

UBC 1st Floor

The Mille

1000 Great West Road

TW89DW

Phone: +44 7397 538 969

E-mail: info@itaassociates.co.uk

www.itaassociates.co.uk

©2025 - All Rights Reserved.