simplilearn

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

96+ hours of instructor-led online classes

Exam voucher included for CEH

64+ hours of e-learning content

Master's Certificate upon course completion

About Simplilearn

Simplilearn is the world's #1 online bootcamp provider that enables learners through rigorous and highly specialized training. We focus on emerging technologies and processes that are transforming the digital world, at a fraction of the cost and time as traditional approaches. Over one million professionals and 2000 corporate training organizations have harnessed our award-winning programs to achieve their career and business 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. **CompTIA Security+ 501**
   52 hrs
3. **Certified Ethical Hacker**
   40 hrs
4. **CISM®**
   16 hrs
5. **CISSP®**
   52 hrs
6. **Certified Cloud Security Professional**
   6 hrs
7. **Masters Certificate**
   You will get individual certificates for each

Electives

- CompTIA Network+

STEP 1 2 3 4 5 6

Introduction to Cyber Security

Simplilearn'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

CompTIA Security+ 501

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

STEP 1 2 3 4 5 6

CEH

The Simplilearn's CEH v10 Certified Ethical Hacker training (earlier CEH v9) 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 practical exam
- 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

CISM®

This CISM certification training from Simplilearn will give you the requisite skill sets to design, deploy and manage security architecture for your organization. The course is aligned with ISACA best practices and is designed to help you pass the CISM exam on your first attempt.

Key Learning Objectives

After completing this phase, you will be able to:

- Define and design security architecture for your IT operation
- Develop a working knowledge of the four domains prescribed by the ISACA Exam Candidate Information Guide 2015
- Demonstrate a deep understanding of the relationship between information security programs and broader business goals and objectives.
- Focus on IT compliance and the integrity of enterprise systems to establish a more secure enterprise IT framework
- Earn the requisite 16 CPEs required to take the CISM certification exam
- Acquire the relevant knowledge and skills required to pass the CISM certification exam

Course Curriculum

- **Lesson 1 -** Information Security Governance - Understand the broad requirements for effective information security governance, the elements and actions required to develop an information security strategy, and be able to formulate a plan of action to implement this strategy.
- **Lesson 02:** Information Risk Management and Compliance - Establish a process for information asset classification and ownership and Identify legal, regulatory, organizational and other applicable requirements to ensure that risk assessments, vulnerability assessments, and threat analysis are conducted periodically.
- **Lesson 03:** Information Security Program Development and Management - Develop and manage an information security plan.
- **Lesson 04:** Information Security Incident Management - Manage information security within an enterprise and develop policies and procedures to respond to and recover from disruptive and destructive information security events.

STEP 1 2 3 4 5 6

CISSP®

Simplilearn'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

STEP 1 2 3 4 5 6

CCSP

Simplilearn's online CCSP training course will help you gain expertise in cloud security architecture, design, applications, and operations. CCSP by ISC2 is a globally acknowledged certification which represents the highest standard for Cloud security. This course provides step by step guidance and easy-to-follow detailed explanation on every facet of CCSP.

Key Learning Objectives

After completing this phase, you will be able to:

- Gain a firm foothold on Cloud computing and relevant security concepts
- Comprehend design principles of secure Cloud computing
- Know about Cloud data lifecycle
- Design Cloud data storage architectures and security strategies, and implement them effectively
- Apply data discovery and classification technologies
- Create and execute relevant jurisdictional data protection for personally identifiable information
- Plan and implement data retention deletion archival policies

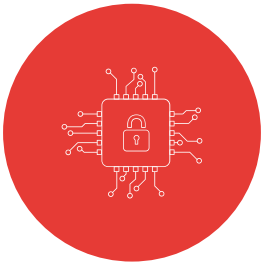
- Learn about Cloud infrastructure components and analyze risks associated with it
- Recognize the need for training and awareness in application security
- Understand Software Development Lifecycle (SDLC) process and apply it
- Frame appropriate Identity and Access Management (IAM) solutions
- Build and run logical and physical architectures for Cloud
- Acquire an understanding of legal requirements, privacy issues, and audit process methodologies within the Cloud environment

Course Curriculum

- **Domain 01:** Architectural concepts and design requirements - Understand cloud computing concepts, cloud reference architecture, design principles of secure cloud computing
- **Domain 02:** Cloud Data Security - Comprehend and apply Cloud Data Lifecycle, data security strategies, data discovery and classification technologies, data rights management, and many more
- **Domain 03:** Cloud Platform and Infrastructure Security - Analyze risks associated to cloud infrastructure, design and plan security controls and disaster recovery
- **Domain 04:** Cloud Application Security - Learn about Software Development Life-cycle(SDLC) process, specifics of cloud application architecture, and many more in this domain
- **Domain 05:** Operations - Build, implement, and manage physical infrastructure for Cloud environment
- **Domain 06:** Legal and Compliance - Understand legal requirements, privacy issues, audit process, cloud contract design

Elective Course

CompTIA Network+

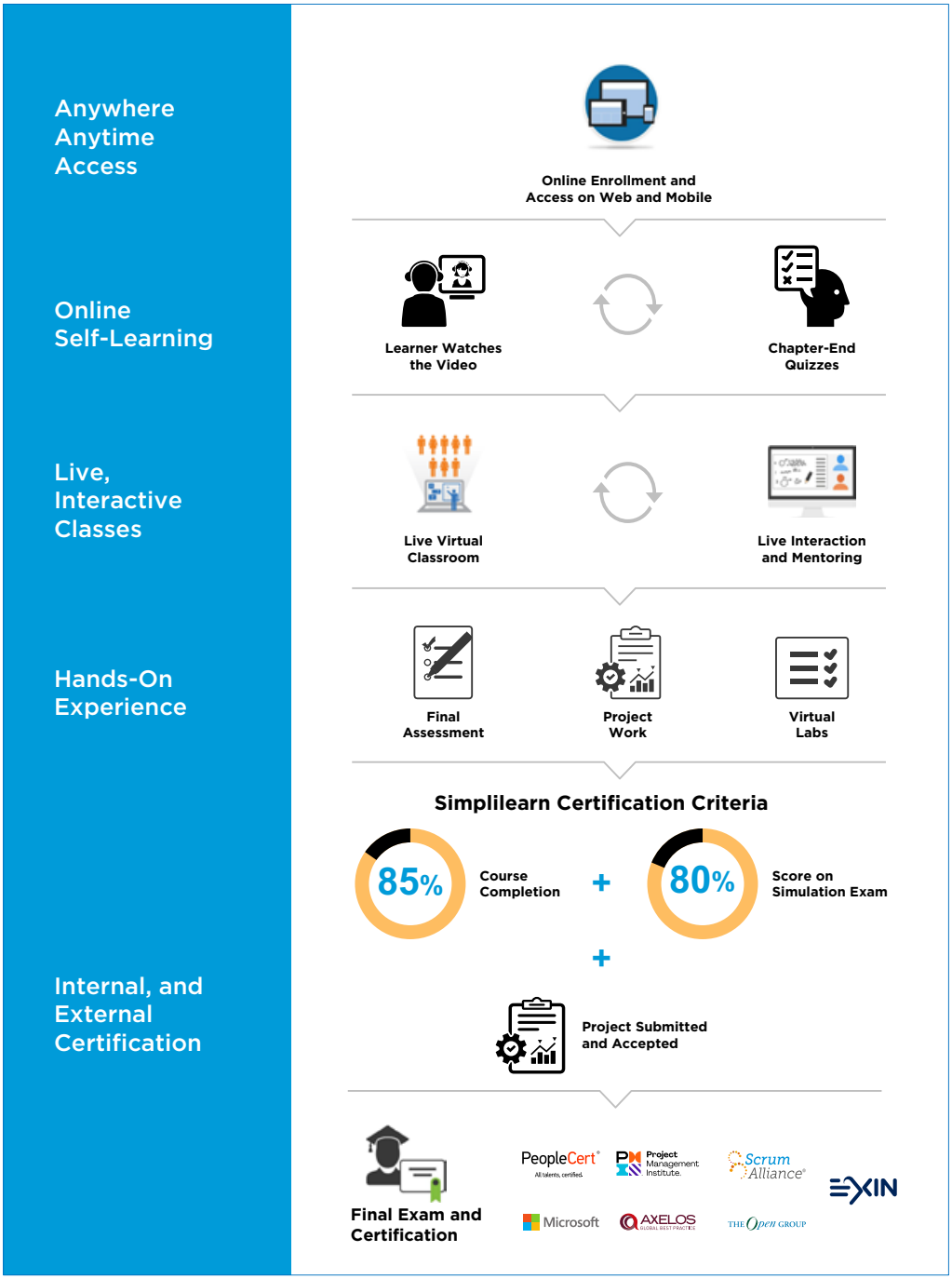


CompTIA Network+ is an ISO-17024 compliant, vendor-neutral technology certification that verifies the skills and knowledge of a certified individual to take on a pivotal role in building, managing, and protecting the critical asset i.e. the data network. The CompTIA Network+ course from Simplilearn covers the objectives of the Network+ exam N10-006 and focuses mainly on the IT skills mostly used by the IT professionals. It also covers topics on troubleshooting, security knowledge, and security controls.

Certificate

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

Classroom-Level Immersion: Delivered Digitally



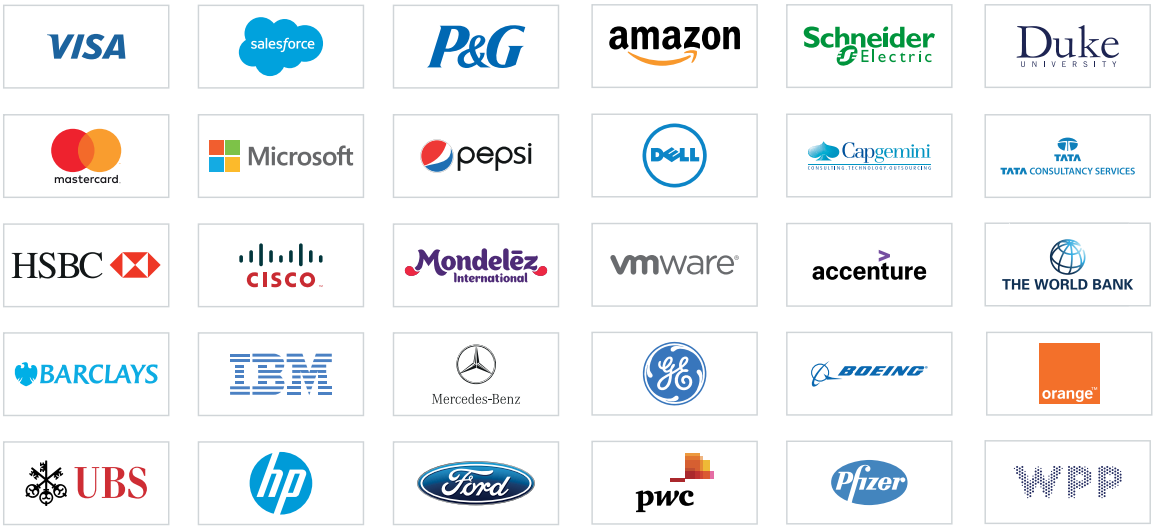
Customer Reviews

Walter Anderson

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

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