Post Graduate Program in

CYBER SECURITY

With Modules from

MIT Schwarzman College of Computing

EC-COUNCIL
CIRCLE OF EXCELLENCE AWARD

Table of Contents

About the Program 3

Key Features of the Post Graduate Program in Cyber Security 4

About the Post Graduate Program in Cyber Security 5

About Simplilearn 6

Program Eligibility Criteria and Application Process 7

Learning Path Visualization 9

Program Outcomes 10

Who Should Enroll in This Program 11

Courses

- **Step 1 :** Introduction to Cybersecurity 12
- **Step 2 :** Design systems to secure applications, networks, & device 13
- **Step 3 :** Build a Hacker MIndset and defend against future attacks (From EC-COUNCIL) 15
- **Step 4 :** Design, engineer and manage the overall security posture of an organization 18
- **Step 5 :** Cybersecurity- Technology, Application and Policy (From MIT Schwarzman College of Computing) 20
- **Step 6 :** Cyber Security Capstone Project 22

Certificates 22

About the Program

Accelerate your career with this Post Graduate Program in Cyber Security. This program features a mix of theory, case studies, and extensive hands-on practice to prepare you for an exciting career in cyber security. You will master CompTIA Security+, CEH, and CISSP, and learn how to protect your infrastructure by securing data and information, running risk analysis, architecting cloud-based security, and achieving compliance.

Key Features of the Post Graduate Program in Cyber Security

Online Classes

110+ hours of instructor-led online classes

Projects

Capstone Project in 3 domains

Content

40 hours of e-learning content

Learning Kit

EC Council Learning Kit

Blended Learning

150+ hours of Blended Learning

Faculty

Masterclasses from MIT Faculty

Certification

- Overall Program Completion: Simplilearn
- 'Cyber Security: Technology, Application and Policy' Module: MIT
- Certified Ethical Hacker: EC Council

Community

MIT CSAIL Professional Programs Community Membership MIT CSAIL Professional Programs Community Membership

About the Post Graduate Program in Cyber Security

This Post Graduate Program in Cyber Security equip you with the skills needed to become an expert in this rapidly growing domain. This program also contains two major modules from MIT SCoC and EC- Council which helps to develop a 360-degree view of the cybersecurity domain that now comprises a wide array of security components and technologies.

About Massachusetts Institute of Technology (MIT) Schwarzman College of Computing:

Founded in 1861, MIT adopted a European polytechnic university model and stressed laboratory instruction in applied science and engineering. It has since played a key role in the development of many aspects of modern science, engineering, mathematics, and technology, and is widely known for its innovation and academic strength, making it one of the most prestigious institutions of higher learning in the world.

MIT also places among the top five in many overall rankings of universities along with Times Higher Education has recognized MIT as one of the world's "six super brands" on its World Reputation Rankings. In 2019, it ranked 3rd among the universities around the world by SCImago Institutions Rankings.In 2017, the Times Higher Education World University Rankings rated MIT the #2 university for arts and humanities. MIT was ranked #7 in 2015 and #6 in 2017 of the Nature Index Annual Tables, which measure the largest contributors to papers published in 82 leading journals.

About EC Council:

The International Council of Electronic Commerce Consultants (EC-Council) is a professional organization that certifies individuals in various e-business and information security skills. EC-Council is best known for its professional certifications for the IT security field. It's certifications CEH,CHFI,CCISO,CND

are ANSI accredited.Many of these certifications are recognized worldwide and have received endorsements from various government agencies including the U.S. Federal Government via the Montgomery GI Bill, National Security Agency (NSA), and the Committee on National Security Systems (CNSS).

Upon completing this program, you will receive:

- The final program completion certificate is from Simplilearn
- Individual course completion certificate for all the courses in learning path from Simplilearn
- Executive Program Certification from MIT
- Certified Ethical Hacker Certificate from EC Council
- MIT CSAIL Professional Programs Community Membership

About Simplilearn

Simplilearn is a leader in digital skills training, focused on the emerging technologies that are transforming our world. Our unique Blended Learning approach drives learner engagement and is backed by the industry's highest course 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 Eligibility Criteria and Application Process

Those wishing to enroll in this Post Graduate Program in Cyber Security will be required to apply for admission.

Eligibility Criteria

For admission to this Post Graduate Program in Cyber Security, candidates:

- Should have a bachelor's degree in any discipline with an average of 50% or higher marks
- With a non-programming background can also apply
- Having prior work experience is not mandatory

Application Process

The application process consists of three simple steps. An offer of admission will be made to the selected candidates and accepted by the candidates upon payment of the admission fee.

STEP 1

Submit an Application

Complete the application and include a brief statement of purpose to tell our admissions counselors why you're interested and qualified for this Post Graduate Program in Cyber Security.

STEP 2

Application Review

After you submit your application, a panel of admissions counselors will review your application and statement of purpose to determine your qualifications and interest in the program.

STEP 3

Admission

An offer of admission will be made to qualified candidates. You can accept this offer by paying the program fee.

Talk to an Admissions Counselor

We have a team of dedicated admissions counselors who are here to help guide you in the application process and related matters. They are available to:

- Address questions related to the application
- Assist with financial aid (if required)
- Help you better understand the program and answer your questions

Learning Path Visualization

1 Introduction to Cybersecurity

2 Design systems to secure applications, networks, & device

3 Build a Hacker MIndset and defend against future attacks (From EC-COUNCIL)

4 Design, engineer and manage the overall security posture of an organization

5 Cybersecurity- Technology, Application and Policy (From MIT Schwarzman College of Computing)

6 Cybersecurity- Capstone Project

7 **PGP Certificate**

Program Outcomes

At the end of this Post Graduate Program,
you will be equipped with the following skillsets:

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

Who Should Enroll in this Program?

This program caters to those who are hoping to enter the world of Cyber Security or want to update their skills, as it is designed and structured to accommodate various professional backgrounds. Although there are no prerequisites for taking this training program, individuals in the following roles and disciplines are ideal 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

STEP
01

Introduction to Cybersecurity

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

Course curriculum

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

STEP
02

Design systems to secure applications, networks, & device

This 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

After completing this course you will be able to:

- 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 -** 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, socialengineering 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 3 - Build a hacker mindset and defend against future attacks (From EC-COUNCIL CIRCLE OF EXCELLENCE AWARD)

This Simplilearn's 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 coverconcepts 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
04

Design, engineer and manage the overall security posture of an organization

This Simplilearn's course 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

After completing this course you will be able to:

- 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
05

Cybersecurity - Technology, application, and policy (From MIT Schwarzman College of Computing)

This course would be conducted by the 15 MIT expert instructor and will target the participants to learn the state-of-the-art in cybersecurity. The course aims to reduce the time from research to industry dissemination and expose the participants to some of the most recent ideas and techniques in cybersecurity.

Key Learning Objectives

After completing this course you will be able to:

- Why building secure systems is so hard, what are the main causes of security breaches, and where do they come from?
- How and where cybersecurity challenges arise in a number of domains
- The “hardware security architecture problem”: how do we think about security when architecting hardware systems
- Operating systems security
- Computational approaches for verifying the security of systems
- Secure programming languages
- Fundamentals of public key cryptography

- New approaches to secure computation: multi-party computing, secret sharing, distributed trust
- New methods for computing on encrypted data
- Network security and protocol design

Course curriculum

- **Lesson 1:** Introduction
- **Lesson 2:** Systems Security
- **Lesson 3:** Cryptography and Network
- **Lesson 4:** Case Studies
- **Lesson 5:** Policy

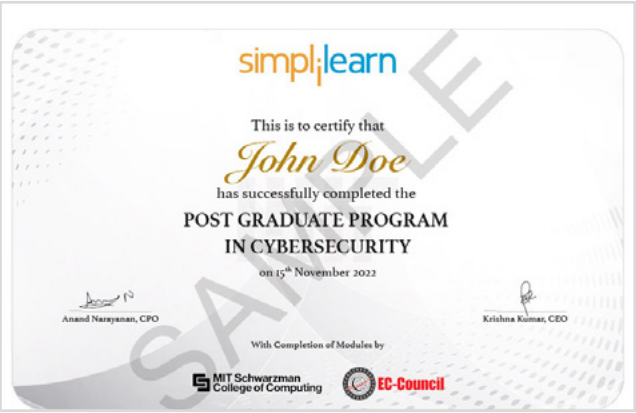
STEP
06

Cyber Security- Capstone Project

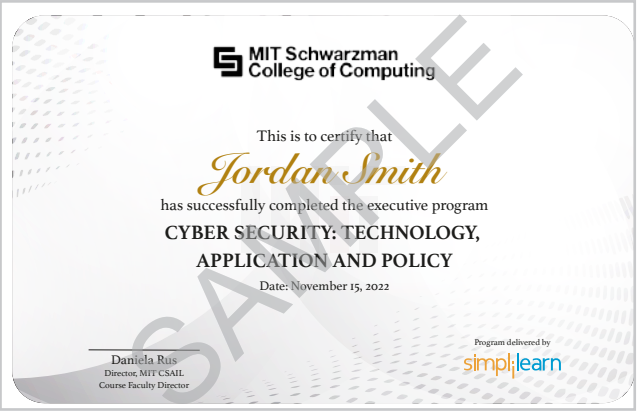
This CyberSecurity capstone project will give you an opportunity to implement the skills you learned throughout this program. Through dedicated mentoring sessions, you'll learn how to solve a real-world, industry-aligned problem. This project is the final step in the learning path and will enable you to showcase your expertise in Cyber Security to future employers.

Certifications

Upon completion of this Post Graduate Program in Cyber Security, you will receive :



1. The Post Graduate Program Certification from Simplilearn



2. The module completion certificate for 'Cyber Security: Technology, Application and Policy' is given by MIT SCC

3. Certified Ethical Hacker certificate from EC Council

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