VIDYA MENTORS

Differentiate yourself - Become a Cyber Security Expert

The Cyber Security Expert Program will help learners develop a deeper understanding of modern information and system protection technology and methods, 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 through industry-leading certification courses, including ISO 27001, CEH, CHFI, CISM, CCSP and CISSP.

What is Cyber crime?

Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials. Cybercriminals may target private personal information, as well as corporate data for theft and resale.

The true cost of cybercrime is difficult to accurately assess. In 2018, McAfee released a report on the economic impact of cybercrime that estimated the likely annual cost to the global economy was nearly $600 billion which is 0.8% of global GDP, and these numbers are considering that only 5% of the cyber crimes are reported. IP theft alone accounts for at least 25% of the cost of cyber crime and threatens national security when it involves military technology. IP theft can be fatal for companies, especially for small and medium-sized businesses.

Currently, more than 6,000 online criminal marketplaces sell ransomware products and services, offering more than 45,000 different products. A cybercriminal group has amassed 1.2 billion username and password combinations and more than 500 million email addresses in last one year.

This makes cybercrime part of a larger problem, as nations undergo the digital revolution that has changed business, politics, security, and law enforcement. Cybercrime will continue to grow as the number of connected devices grows and as the value of online activities increases.

What is the need for Cyber Security?

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security. A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber attacks.

As per NTT Data Security report, during 2018, there was a 12.5% increase in the number of new vulnerabilities discovered. Some 24% of organisations cite a lack of understanding of their current risk profile as a barrier to deploying better security systems. Cryptojacking detections have increased by a staggering 459%. It's now more important than ever to adapt a business-outcome driven approach to tackle cybersecurity and compliance challenges. Some 71% of organisations believe security is important to the organisation's digital strategy and ranked it important of all technologies.

Duration

3 - 5 Months (180 - 300 hours), Integrated Program

Time commitment for candidates – 12-15 hours per week

Eligibility Criteria

0-3 years of work experience

Key highlights

1 Industry recognized trainers

2 One-on-one discussion and feedback sessions

3 Hands-on learning and Hackathons

4 Edge-of-your-seat online learning

5 Global peer collaboration and networking

6 Capstone Project and Live Projects

7 Live sessions by experts on various industry topics

8 Real-world, case-based learning

9 Job assistance, Placement drives

Course Structure and Curriculum

Networking Concepts	Networking Standards and the OSI Model, Transmission Basics and Networking Media, Introduction to TCP/IP Protocols, Topologies and Ethernet Standards, Network Hardware, WANs and Remote Connectivity, Wireless Networking
Security Fundamentals	Risk management, Cryptography, Authentication and authorization, Host, LAN, and application security, Wireless, cloud, and mobile security, Environmental security and controls
Cryptography	Symmetric Cryptosystems, Symmetric Block Modes, RSA Cryptosystems, Diffie-Hellman, PGP/GPG, Hashing, HMAC, Steganography, Certificates and Trust, Public Key Infrastructure, Cryptographic Attacks
Information Security (ISMS - ISO 27001)	Key concepts and principles in ISO/IEC 27001, Business Impact Analysis and Risk management, Infrastructure security, IT security, Understand the approaches, standards, methods and techniques used for the implementation and management of an ISMS, plan, implement, manage, monitor and maintain an ISMS
Risk Management (RMS - ISO 31000)	8 Principles of Risk Management, 31000 Framework, Risk Assessment, Risk treatment, Risk management process, Checklist
Security Management (CISM)	Information Security Governance, Information Risk Management and Compliance, Information Security Program Development, Information Security Incident Management, Security Teams Management
Information Systems Security Professional (CISSP)	Confidentiality, Integrity, and Availability (CIA), Security Policy Implementation, Asset Security, Security Engineering, Communications and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, Software Development Security

Cloud Security (CCSP)	Cloud Concepts, Architecture and Design, Cloud Data Security, Cloud Platform & Infrastructure Security, Cloud Application, Cloud Security Operations, Legal, Risk and Compliance
Ethical Hacking & VAPT (CEH)	Introduction to Ethical Hacking, Footprinting and Reconnaissance, Scanning Networks, Enumeration, Vulnerability Analysis, System Hacking, Malware Threats, Sniffing, Social Engineering, Denial-of-Service, Session Hijacking, Evading IDS, Firewalls, and Honeypots, Hacking Web Servers, Hacking Web Applications, SQL Injection, Hacking Wireless Networks, Hacking Mobile Platforms, IoT Hacking
Security Operations(SOC)	Business orientation, use case development, hunting techniques Functions of a SOC: monitoring, response, intelligence, metrics Internal capability development and strategic outsourcing Technology, process, and staff optimization, Steps to build a SOC, or assess an established SOC's maturity
Live Projects	As per the requirements from the industry

Why Cyber Security Expert?

The shortage of skilled and qualified cybersecurity professionals is one of the biggest issue, the Internet-connected world is facing today. As smart technology advances, the ways in which our lives can be greatly impacted by cybercrime increase dramatically.

Security is a crucial domain in any organization. Cybersecurity Ventures predicts there will be 3.5 million cybersecurity job openings by 2021. The National Association of Software and Services Companies (NASSCOM) recently estimated that India alone will need 1 million cybersecurity professionals by 2020 to meet the demands of its rapidly growing economy. Cybersecurity experts must learn to develop a 360-degree view of the cybersecurity domain that now comprises a wide array of security components and technologies.

Program Objectives

At the end of this 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 data storage architectures, security strategies, and utilize them to analyze risks
- Protect data movement, perform disaster recovery, access CSP security and manage client databases

Program Structure

Cyber Security Expert Program uses a combination of learning methods that include classroom teaching, Video based training, hands-on exercises, and sessions with industry experts

- Classroom training
- Video-led training
- Lab sessions

Jobs and Profiles related to Cyber Security

Jobs and Profiles related to Cyber Security

Penetration tester/Assurance Validator	Chief Information Security Officer
Cybersecurity analyst	Information Security Analyst
Network analyst	Security Architect
Cybersecurity auditor	Security Engineer
Cybersecurity architect	Security Systems Administrator
Forensics investigator	Security Consultant
Cryptographer/Cryptologist	Vulnerability Assessor

What is Job Assistance?

- Resume Building Assistance
- Career Mentoring
- Interview Preparation