Unleash Your Cybersecurity Potential:

Defend, Secure, Thrive

SevenMentor PVT.LTD

www.sevenmentor.com

Cyber Security Course Mission

Empowering guardians of the digital realm, our cybersecurity program is on a mission to forge defenders armed with cutting-edge knowledge. We strive to mold experts who not only outsmart cyber threats but also champion ethical practices. Through dynamic learning and hands-on experiences, our program seeks to create a resilient cohort capable of navigating the ever-changing landscape of cybersecurity. Join us in shaping a secure digital future."

Defend. Ethical. Resilient.

CYBER SECURITY STATISTICS:

INDUSTRY INSIGHTS

85% Servers across the world have security vulnerabilities waiting to be exploited by malicious actors

31% Unfulfilled Vacancies since 2020 throughout India

3.5X Growth in hiring for Cyber Security experts and consultants in major MNCs.

Security never goes out of style

Embrace the power of cybersecurity education, where every skill learned becomes a shield against evolving threats. In a digital age, being in demand is about securing the virtual frontiers. Equip yourself with cybersecurity expertise, ensuring you're not just sought after today but are a guardian of tomorrow's digital landscape.

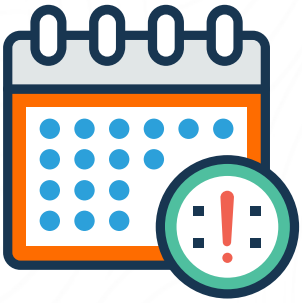
Become an CyberSecurity Analyst

Embark on a transformative journey to become the cybersecurity analyst you aspire to be. Equip yourself with cutting-edge skills, analyze threats, and safeguard digital landscapes. Your path to cybersecurity excellence starts here.Dive into the dynamic realm of cybersecurity as you shape your destiny to become the sought-after cybersecurity analyst. Uncover the intricacies of threat analysis, fortify digital defenses, and emerge as a guardian of cyber landscapes. Your journey to mastery begins now, charting a course to a future where security meets expertise

Be Prepared For Every Scenario!

SevenMentor Institute offers a comprehensive range of courses to help you learn the skills you need to protect data and systems from attack from every type of attack. Our Cyber Security Course in Pune is designed for beginners and experienced professionals alike, and we offer both online and in-person training options.

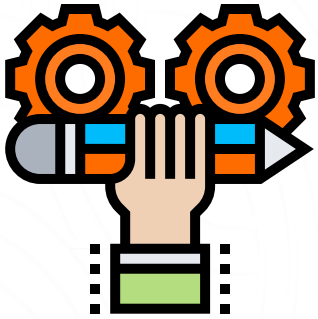
Experienced Faculty



Flexible Scheduling

Hands-On Learning

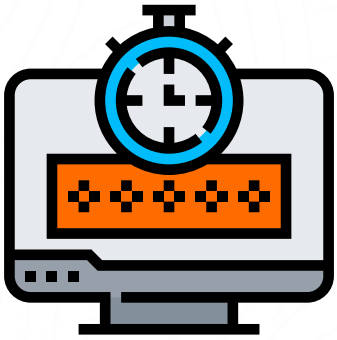
Mock Interview Sessions



Real-World Projects

Career Support

Comprehensive Curriculum



Lifetime Access

CCNA

Network Fundamentals

1.1 Explain the role and function of network components
1.1.a Routers
1.1.b L2 and L3 switches
1.1.c Next-generation firewalls and IPS
1.1.d Access points
1.1.e Controllers (Cisco DNA Center and WLC)
1.1.f Endpoints
1.1.g Servers
1.2 Describe characteristics of network topology architectures
1.2.a 2 tier
1.2.b 3 tier
1.2.c Spine-leaf
1.2.d WAN
1.2.e Small office/home office (SOHO)
1.2.f On-premises and cloud
1.3 Compare physical interface and cabling types
1.3.a Single-mode fiber, multimode fiber, copper
1.3.b Connections (Ethernet shared media and point-to-point)
1.3.c Concepts of PoE
1.4 Identify interface and cable issues
(collisions, errors, mismatch duplex, and/or speed)
1.5 Compare TCP to UDP
1.6 Configure and verify IPv4 addressing and subnetting
1.7 Describe the need for private IPv4 addressing
1.8 Configure and verify IPv6 addressing and prefix
1.9 Compare IPv6 address types
1.9.a Global unicast
1.9.b Unique local
1.9.c Link local
1.9.d Anycast
1.9.e Multicast
1.9.f Modified EUI 64
1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux)
1.11 Describe wireless principles
1.11.a Nonoverlapping Wi-Fi channels
1.11.b SSID
1.11.c RF
1.11.d Encryption
1.12 Explain virtualization fundamentals (virtual machines)
1.13 Describe switching concepts
1.13.a MAC learning and aging
1.13.b Frame switching
1.13.c Frame flooding
1.13.d MAC address table

Network Access

2.1 Configure and verify VLANs (normal range) spanning multiple switches
2.1.a Access ports (data and voice)
2.1.b Default VLAN
2.1.c Connectivity
2.2 Configure and verify interswitch connectivity
2.2.a Trunk ports
2.2.b 802.1Q
2.2.c Native VLAN
2.3 Configure and verify Layer 2 discovery protocols
(Cisco Discovery Protocol and LLDP)
2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations
2.5.a Root port, root bridge (primary/secondary), and other port names
2.5.b Port states (forwarding/blocking)
2.5.c PortFast benefits
2.6 Compare Cisco Wireless Architectures and AP modes
2.7 Describe physical infrastructure connections of WLAN components
(AP, WLC, access/trunk ports, and LAG)
2.8 Describe AP and WLC management access connections
(Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS)
2.9 Configure the components of a wireless LAN access for client connectivity using GUI onlysuch as WLAN creation, security settings, QoS profiles, and advanced WLAN settings

IP Connectivity

3.1 Interpret the components of routing table
3.1.a Routing protocol code
3.1.b Prefix
3.1.c Network mask
3.1.d Next hop
3.1.e Administrative distance
3.1.f Metric
3.1.g Gateway of last resort
3.2 Determine how a router makes a forwarding decision by default
3.2.a Longest match
3.2.b Administrative distance
3.2.c Routing protocol metric
3.3 Configure and verify IPv4 and IPv6 static routing
3.3.a Default route
3.3.b Network route
3.3.c Host route
3.3.d Floating static
3.4 Configure and verify single area OSPFv2
3.4.a Neighbor adjacencies
3.4.b Point-to-point
3.4.c Broadcast (DR/BDR selection)
3.4.d Router ID
3.5 Describe the purpose of first hop redundancy protocol

IP Services

4.1 Configure and verify inside source NAT using static and pools
4.2 Configure and verify NTP operating in a client and server mode
4.3 Explain the role of DHCP and DNS within the network
4.4 Explain the function of SNMP in network operations
4.5 Describe the use of syslog features including facilities and levels
4.6 Configure and verify DHCP client and relay
4.7 Explain the forwarding per-hop behavior
(PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping)
4.8 Configure network devices for remote access using SSH
4.9 Describe the capabilities and function of TFTP/FTP in the network

Security Fundamentals

5.1 Define key security concepts
(threats, vulnerabilities, exploits, and mitigation techniques)
5.2 Describe security program elements
(user awareness, training, and physical access control)
5.3 Configure device access control using local passwords
5.4 Describe security password policies elements, such as management, complexity, and password alternatives
(multifactor authentication, certificates, and biometrics)
5.5 Describe remote access and site-to-site VPNs
5.6 Configure and verify access control lists
5.7 Configure Layer 2 security features
(DHCP snooping, dynamic ARP inspection, and port security)
5.8 Differentiate authentication, authorization, and accounting concepts
5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)
5.10 Configure WLAN using WPA2 PSK using the GUI

Automation and Programmability

6.1 Explain how automation impacts network management
6.2 Compare traditional networks with controller-based networking
6.3 Describe controller-based and software defined architectures
(overlay, underlay, and fabric)
6.3.a Separation of control plane and data plane
6.3.b North-bound and south-bound APIs
6.4 Compare traditional campus device management with Cisco DNA Center enabled device
6.5 Describe characteristics of REST-based APIs
(CRUD, HTTP verbs, and data encoding)
6.6 Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible
6.7 Interpret JSON encoded data

LINUX

RH124 - Red Hat System Administration I

- Accessing the Command Line
- Managing Files from the Command Line
- Getting help in Red Hat Enterprise Linux
- Creating, Viewing and Editing Text Files
- Managing Local Linux Users and Groups
- Controlling Access to Files
- Monitoring and Managing Linux Processes
- Controlling Services and Daemons
- Configuring and Securing OpenSSH Service
- Analyzing and Storing Logs
- Managing Red Hat Enterprise Linux Networking
- Archiving and Copying Files Between Systems
- Installing and Updating Software Packages
- Accessing Linux File Systems
- Analyzing Servers and Getting Suppor

Rh134 - Red Hat System Administration II

- Installing Red Hat Enterprise Linux
- Improving Command Line Productivity
- Scheduling Future Linux Tasks
- Managing Priority of Linux Processes
- Controlling Access to Files With Access Control Lists (ACLs)
- Managing SELinux Security
- Maintaining Basic Storage
- Managing Logical Volume Management (LVM) Storage
- Implementing Advanced Storage Features
- Accessing Network Storage with Network File System (NFS)
- Controlling and Troubleshooting the Red Hat Enterprise Linux Boot Process
- Managing Network Security

RH294 - Red Hat System Administration III

- Introduction to Ansible
- Deploying Ansible
- Implementing Playbooks
- Managing Variables and Facts
- Implementing Task Control
- Deploying Files to Managed Hosts
- Managing Large Projects
- Simplifying Playbooks with Roles
- Troubleshooting Ansible
- Automating Linux Administration Tasks

PYTHON

Session 1: Introduction To Python

- What are Python and the hist
- Ory of Python?
- Unique features of Python
- Python-2 and Python-3 differences
- Install Python and Environment Setup
- First Python Program
- Python Identifiers, Keywords, and Indentation
- Comments and document interlude in Python
- Command-line arguments
- Getting User Input
- Python Data Types
- What are the variables?
- Python Core objects and Functions
- Number and Maths
- Week 1 Assignments

Session 2: Control Statements

- If-else
- If-elif-else
- While Loop
- For Loop
- Break
- Continue
- Assert
- Pass
- Return

Session 3: List, Ranges & Tuples in Python

- Introduction
- Lists in Python
- More about Lists
- Understanding Iterators
- Generators, Comprehensions and Lambda Expressions
- Introduction
- Generators and Yield
- Next and Ranges
- Understanding and using Ranges
- More About Ranges
- Ordered Sets with tuples

Session 4: Python Dictionaries and Sets

- Introduction to the section
- Python Dictionaries
- More on Dictionaries
- Sets
- Python Sets Examples

Session 5: Input and Output in Python

- Reading and writing text files
- Writing Text Files
- Appending to Files and Challenge
- Writing Binary Files Manually
- Using Pickle to Write Binary Files

Session 6: Python built-in function

- Python user-defined functions
- Python packages functions
- Defining and calling Function
- The anonymous Functions
- Loops and statement in Python
- Python Modules & Packages

Session 7: Python Object Oriented

- Overview of OOP
- The self variable
- Constructor
- Types Of Variables
- Namespaces
- Creating Classes and Objects
- Inheritance
- Types of Methods
- Instance Methods Static Methods Class Methods
- Accessing attributes
- Built-In Class Attributes
- Destroying Objects
- Abstract classes and Interfaces
- Abstract Methods and Abstract class
- Interface in Python
- Abstract classes and Interfaces

Session 8: Exceptions

- Errors in Python
- Compile-Time Errors
- Runtime Errors
- Logical Errors
- What is Exception?
- Handling an exception
- try-finally clause
- The argument of an Exception
- Python Standard Exceptions
- Raising an exceptions
- User-Defined Exceptions

Session 9: Python Regular Expressions

- What are regular expressions?
- The match Function
- The search Function
- Matching vs searching
- Search and Replace
- Extended Regular Expressions
- Wildcard

Session 10: Python Multithreaded Programming

- What is multithreading?
- Difference between a Process and Thread
- Concurrent Programming and GIL
- Uses of Thread
- Starting a New Thread
- The Threading Module
- Thread Synchronization
- Locks
- Semaphore
- Deadlock of Threads
- Avoiding Deadlocks
- Daemon Threads

Session 11: Using Databases in Python

- Python MySQL Database Access
- Install the MySQLdb and other Packages
- Create Database Connection
- CREATE, INSERT, READ Operation
- DML and DDL Operation with Database
- Graphical User Interface
- GUI in Python
- Button Widget
- Label Widget
- Text Widget

Session 12: Django Web Framework in Python

- Introduction to MVC and MVT architecture on web development.
- Django folder structure flow of control.

C|EH Certification

Course Outline20 Modules That Help You Master the Foundations of Ethical Hacking

Introduction to Ethical Hacking :

Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Foot Printing and Reconnaissance :

Learn how to use the latest techniques and tools to perform foot printing & reconnaissance, a critical pre-attack phase of the ethical hacking process.

Scanning Networks :

Learn different network scanning techniques and countermeasures

Enumeration :

Learn various enumeration techniques, such as Border Gateway Protocol (BGP) & Network File Sharing (NFS) exploits, & associated countermeasures

Vulnerability Analysis :

Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools.

System Hacking :

Learn about the various system hacking methodologies— including ste-ganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.

Malware Threats :

Learn different types of malware (Trojan, virus, worms, etc.), APT and fileless malware, malware analysis procedure, and malware countermeasures.

Sniffing :

Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

Social Engineering :

Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.

Denial-of-Service :

Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

Session Hijacking :

Understand the various session hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

Evading IDS, Firewalls, and Honeypots :

Get introduced to firewall, intrusion detection system (IDS), & honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.

Hacking Web Servers :

Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

Hacking Web Applications :

Learn about web application attacks, including a comprehensive web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.

SQL Injection

Learn about SQL injection attacks, evasion techniques, and SQL injection countermeasures.

Hacking Wireless Networks

Understand different types of wireless technologies, including encryption, threats, hacking methodologies, hacking tools, Wi-Fi sedcurity tools, and countermeasures.

Hacking Mobile Platforms :

Learn Mobile platform attack vector, android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

IoT and OT Hacking

Learn different types of IoT and OT attacks, hacking methodology, hacking tools, and countermeasures.

Cloud Computing

Learn different cloud computing concepts, such as container technologies and server less computing, various cloudcomputing threats, attacks, hacking methodology, and cloud security techniques and tools.

Cryptography

Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.

WAPT

Introduction to Web Applications

- 1.0 HTTP/S Protocol Basics
- 2.0 Encoding
- 3.0 Same Origin
- 4.0 Cookies
- 5.0 Sessions
- 6.0 Web Application Proxies by using BURP SUIT AND OWASP ZAP

Information Gathering

- 1.0 Gathering information on your target
- 2.0 Infrastructure
- 3.0 Fingerprinting frameworks and applications
- 4.0 Fingerprinting custom applications
- 5.0 Enumerating resources
- 6.0 Relevant information through misconfigurations
- 7.0 Google hacking
- 8.0 Shodan HQ/li>

Cross-Site Scripting

- 1.0 Cross-Site Scripting
- 2.0 Anatomy of an XSS Exploitation
- 3.0 The three types of XSS
- 4.0 Finding XSS
- 5.0 XSS Exploitation
- 6.0 Mitigation

SQL Injection

- 1.0 Introduction to SQL Injections SQLi
- 2.0 Finding SQL Injections
- 3.0 Exploiting Error-based SQL Injections
- 4.0 Exploiting blind SQLi
- 5.0 Finding SQL through Tools
- 6.0 Mitigation Strategies

Authentication & Authorization

- 1.0 Introduction
- 2.0 Common Vulnerabilities
- 3.0 Bypassing Authorization

Session Security & CSRF

- 1.0 Weaknesses of the session identifier
- 2.0 Session hijacking
- 3.0 Session Fixation
- 4.0 Cross-Site Request Forgeries

Remote code execution

- 1.0 Introduction
- 2.0 Remote code Attack
- 3.0 Mitigation Strategies

HTML5

- 1.0 Cross-Windows Messaging
- 2.0 Web Storage
- 3.0 WebSocket
- 4.0 Sandboxed frames

File and Resource Attacks

- 1.0 File Inclusion Vulnerabilities
- 2.0 Unrestricted File Upload

Other Attacks

- 1.0 Command Injection
- 2.0 Price Manipulation
- 3.0 OTP BYPASSING
- 4.0 Denial of Services

Web Services

1.0 Introduction
2.0 Web Services
3.0 The WSDL Language
4.0 Attacks

Xpath Injection

- 1.0 XPath & XPath expression & syntax
- 2.0 Detecting XPath
- 3.0 Best Defensive Techniques

Penetration Testing Content Management Systems

- 1.0 Introduction
- 2.0 WordPress
- 3.0 Joomla
- 4.0 Brute Force Attack Through WP

Penetration Testing NoSQL Databases

- 1.0 Introduction
- 2.0 NoSQL Fundamentals & Security
- 3.0 NoSQL Exploitation

SOC

Module 1 : SOC Essential Concepts

- Basics of Networking and Security Concepts
- Types of IP address How Computer Communication.
- Transport Protocol IP Planning.
- DNS Server and Various types of DNS records.
- Understanding of OSI model and Reference layer devices.
- TCP/IP Packet Understanding. 3 Ways Handshake.
- Router, Switches And designing Corporate network etc.
- Understanding of Firewall. Web Application Firewall (WAF) Proxy
- Email Gateway (Email Security)
- Network ATTACK

Module 2 : Security Operations and Management

- Security Management
- Security Operations
- Security Operations Center (SOC)
- Need of SOC
- SOC Capabilities
- SOC Operations
- SOC report
- Kill Chain Deep Dive Scenario - Spear Phishing

Module 03: Understanding Cyber Threats & Attack Methodology

- Cyber Threats
- Tactics-Techniques-Procedures (TTPs)
- Opportunity-Vulnerability-Weakness
- Network Level Attack
- Application Level Attacks
- SQL Injection Attacks
- Email Security Threats

Module 04 : Incidents, Events, and Logging

- What is the mean of Log
- What is incidents and event
- Local Logging : windows and linux logs
- How to get ROUTER AND WEB SERVER LOGS
- WHAT is Centralized Logging
- Why we need a logs
- Deeply log analysis
- Alerting and reporting

Module 05: Incident Detection with Security Information and Event Management (SIEM)

- Security Information and Event Management(SIEM)
- Need of SIEM
- Typical SIEM Capabilities
- SIEM Architecture and Its Components
- Splunk Enterprise Security
- Nessus
- SIEM Deployment
- Incident Detection with SIEM
- Handling Alert Triaging and Analysis

Module 6: Incident Detection with Threat Intelligence

- Understanding Cyber Threat Intelligence
- How can Threat Intelligence Help Organizations?
- Threat Intelligence Strategy
- Threat Intelligence Sources: OSINT

Module 07: Incident Response

- Incident Response (IR) Process Overview
- SOC and IRT collaboration
- Responding to Network Security Incident
- Responding to Application Security Incidents
- Responding to Email Security Incidents
- Responding to an Insider Incidents

CHFI

Introduction

- 1.0 Computer Forensics In Today's World
- 1.0 Intro To Computer Forensics
- 2.0 Need For Computer Forensics
- 3.0 What is Cyber Crime
- 4.0 Forensics Investigation Process
- 5.0 Cyber Law

Understanding Hard Disks and File systems

- 1.0 Disk Drive Overview
- 2.0 Booting Process
- 3.0 Windows File Systems
- 4.0 Linux File Systems
- 5.0 Mac File Systems
- 6.0 The Sleuth Kit (TSK) And Autopsy

Defeating Anti-Forensics Techniques

- 3.0 Password Cracking System and Application
- 4.0 Cracking BIOS Password
- 5.0 Alternate Data Stream
- 6.0 Encrypted File System

Network Forensics

- 1.0 Network Forensic
- 2.0 Intrusion Detection System (IDS)
- 3.0 Firewall, IPS and Reverse-Proxy
- 4.0 Honeypot And Tracing
- 5.0 Traffic Capturing and Analysis

Database Forensics

- 1.0 Logon event in Windows and Linux
- 2.0 Syslog Identification
- 3.0 Log Capturing and Analysis

Computer Forensics Investigation Process

- 1.0 Forensic Workstation Building SIFT
- 2.0 Chain of Custody
- 3.0 Data Imaging(FTK Imager)
- 4.0 Data Integrity(sha256sum)
- 5.0 Data Carving(Physical Level)
- 6.0 Data Analysis(FTK Toolkit)
- 7.0 Expert witness
- 8.0 PCI-DSS, DMCA, FISMA ACT

Data Acquisition and Duplication

- 1.0 Static and Live Acquisition
- 2.0 Volatile Information from Linux & Windows
- 3.0 Acquiring Data on Windows
- 4.0 Acquiring Data on Linux
- 5.0 FTK Imager and ddclfd (Bit-Stream copy)
- 6.0 Netcat for Forensic

Operating System Forensics

- 1.0 Network and Process Information
- 2.0 Cache, Cookie and History Analysis
- 3.0 Registry Analysis
- 4.0 Linux Configuration Analysis
- 5.0 Windows Event Viewer

Investigating Web Attacks

- 1.0 Network Forensic
- 2.0 Intrusion Detection System (IDS)
- 3.0 Firewall, IPS and Reverse-Proxy
- 4.0 Honeypot And Tracing
- 5.0 Traffic Capturing and Analysis

Cloud Forensic

- 1.0 What is cloud.
- 2.0 What is Reverse-Proxy
- 3.0 Squid Configuration
- 4.0 Log Analysis using Grep,awk,date,etc.

Malware Forensic

- 1.0 Unstructured Memory Analysis
- 2.0 Bulk Extractor
- 3.0 cridex malware identification
- 4.0 Network Activity to a Process

Investigating Email Crimes

- 1.0 Email System Architecture
- 2.0 Email Crimes
- 3.0 Email Header Analysis
- 4.0 Tracing Emails

Mobile forensic

- 1.0 Mobile Device
- 2.0 Cellular Network
- 3.0 Knowledge of Mobile forensics tools
- 4.0 Mobile Forensic Process
- 5.0 Mobile Forensic Reports (Real time)

Forensics report writing and presentation

- 1.0 Forensics Report
- 2.0 Report Writing And Documentation
- 3.0 Sample Report Writing
- 4.0 Writing Reports using FTK
- 5.0 Writing Reports using Autopsy

Case Studies

Get Skills To Fulfill Every Role:

Every student at **SevenMentor** gets personalized guidance, Mentorship, and ample opportunities to address individual questions and concerns. All our sessions are designed to be engaging, interactive, and tailored to your learning pace, ensuring you grasp each concept with clarity.

Samir S.khatib

He is currently working at **SevenMentor Pvt ltd** Pune as Networking and Cloud Trainer. Samir is working as technical trainer since 2002. He have relevant experience of 20 years as trainer, which includes Industrial experience as well. Samir has been training for Microsoft server technology, Networking technology like Cisco CERTIFICATION, and Cloud Computing. Samir is certified with global certification by CISCO, MICROSOFT. Samir is Bachelor in Information Technology (B. Tech). His area of interest are CISCO, MICROSOFT, and CLOUD COMPUTING.

Rajat Sharma

currently working at Sevenmentor pvt ltd Pune as Cyber Security & Cloud Trainer. Rajat is working as cyber security trainer since 20017. He have relevant experience of 6 years as trainer, which includes Industrial experience as well. Rajat has been training for Cyber security, web application penetration testing, SOC Training and Cloud Computing. Rajat is certified with global certification by Ec-Counsil and AWS. Rajat is master in LAW. His area of interest are Cybersecurity & Cloud Security

Abhijeet Dahatonde

Abhijeet is a graduate in Information Technology Engineering[BE.IT], Post graduate in IT [MBA-IT]and also Cyber law certified from symbiosis University, International Certified in Cyber Security, Linux Administrator, Windows Administrator, Cisco, CompTIA Global Certifications. Being a Cyber Security Researcher, Forensic Researcher and Ethical Hacking Expert, Abhijeet has revealed numerous critical vulnerabilities, bugs, loop holes, etc on websites and networks of major corporate and institutions. Currently members of various underground hacking groups, security researchers and communities worldwide. His fanaticism for Security, Sys Adminstration, Programming and Cloud made him expert in the security,server administration,cloud,DevOps domain.

Get Skills To Fulfill Every Role:

Our Cyber Security Courses are designed for a wide range of people looking for skills and opportunities across all major Cyber Security sectors

Threat Analysis: Understanding the different types of cyberattacks and how they work.

Vulnerability Assessment: Identifying and fixing vulnerabilities in systems and networks.

Incident Response: How to respond to a security incident & minimize damage.

Risk Management: Understanding & mitigating the risks to your data & systems.

Our Students are at reputed Tech Companies

BAJAJ FINSERV · GT FINANCIAL SERVICES · INFERYX · STRELEMA · pivotchain · LONAR TECHNOLOGIES

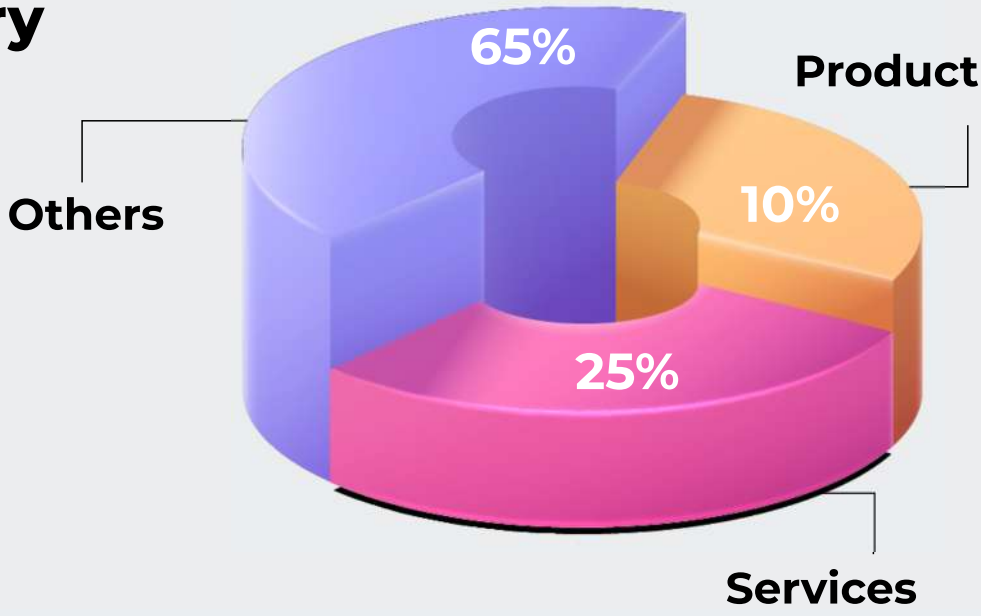
Simplify Healthcare · OMFYS · Scymes · KALA Genset Source of Power · Altum Credo Home Finance · INFOWORLD THE SOFTWARE PEOPLE

NABLA INFOTECH · Circulants · SRV media Insights | Ideas | Impact · Rabbit&Tortoise TECHNOLOGY SOLUTIONS · NIMAP INFOTECH · Integs Cloud

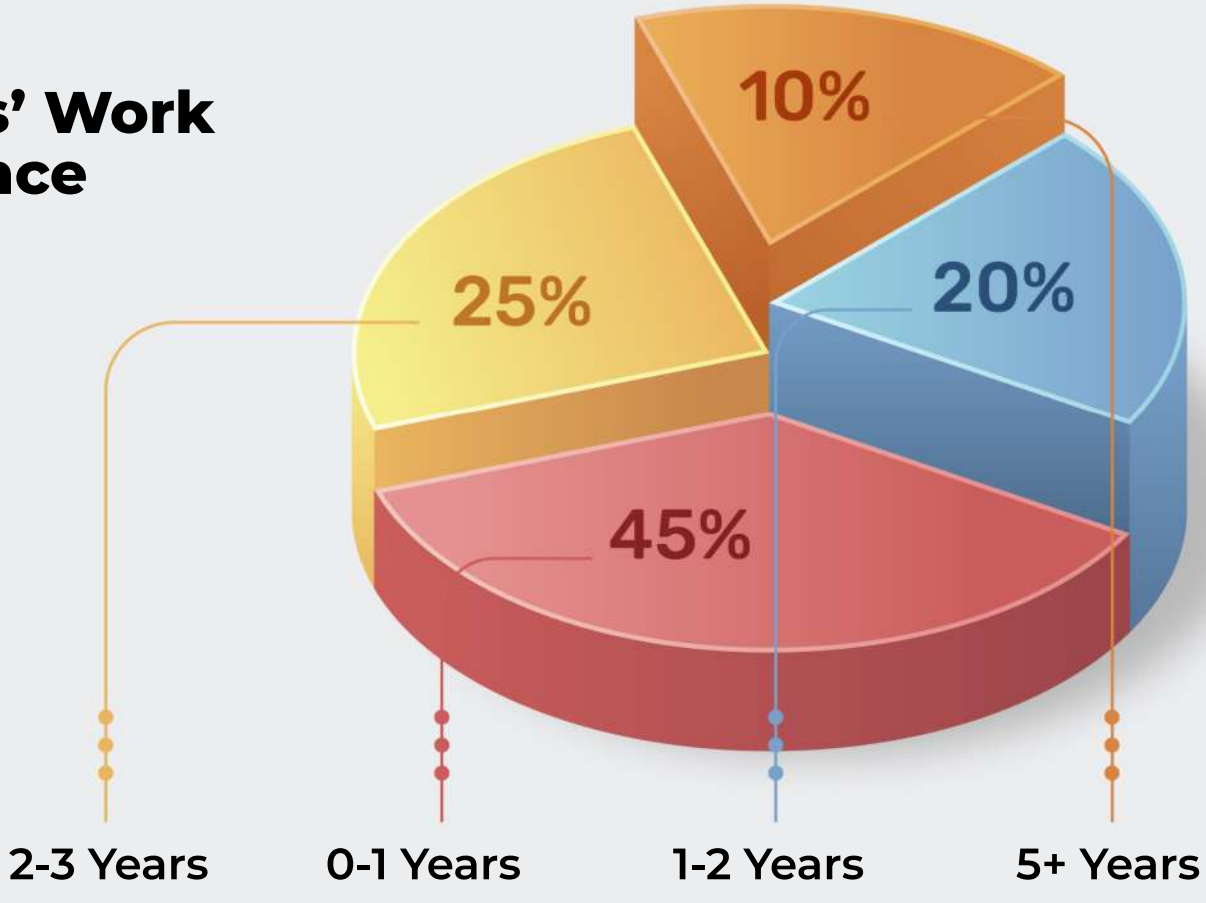
Cyber Security Jobs are also very Stable!

The demand for Cyber Security professionals is growing rapidly, so there is a lot of job security in this field. This can be a great motivator for people who are looking for a stable career.

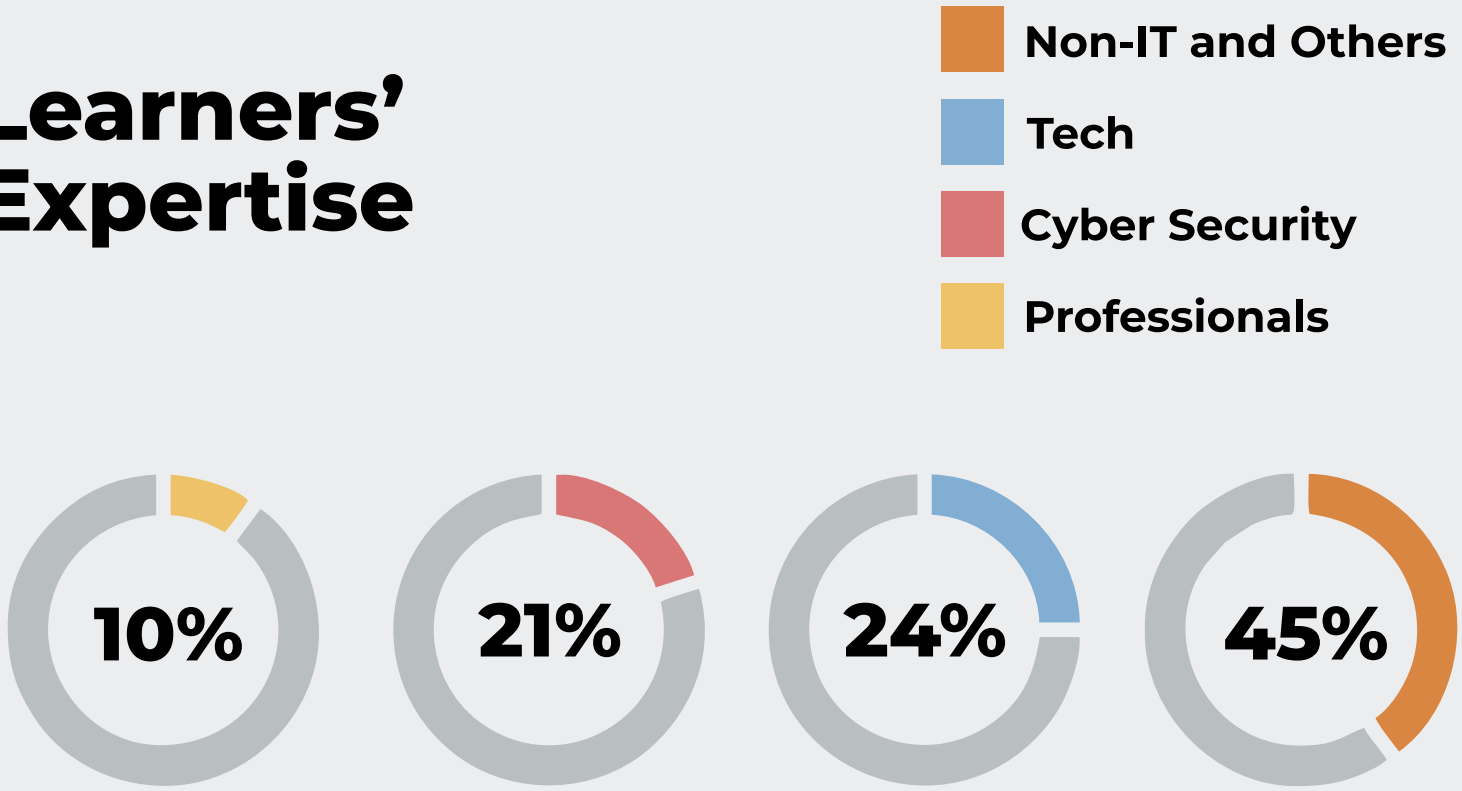
Learners' Industry Background



Learners' Work Experience



Learners' Expertise



BOOST YOUR CAREER TO NEW HEIGHTS:

The global Cyber Security job market is expected to grow by 44% from 2021 to 2030, creating 3.5 million new jobs.
In India it is expected that 309,000 new Cyber Security jobs will be available by 2030, accounting for 9% of the global demand. The average salary for a Cyber Security professional in India is approximately Rs. 14 Lakhs per annum.

Preparing Young Minds to Tackle Large Threats:

SevenMentor Institute is passionate about teaching and helping students learn about Cyber Security. We believe that everyone should have the knowledge they need to protect themselves and their organizations from cyber attacks. We are therefore excited to deliver knowledge and experience with you and help you become a Cyber Security expert. We request you to take a demo course with us and have a glimpse of this fascinating realm of Cyber Security.

HOW TO START YOUR CYBER SECURITY CAREER?

- Gain skills through **Internships and Real-world Projects** at SevenMentor.
- Earn a recognized Cyber Security **Certification** from SevenMentor Institute
- Receive Job Offers from **MNCs** across India

WE ARE THERE FOR YOU

If you are interested in learning more about Cyber Security training, please contact us. Our team would be happy to answer any questions you have and help you find the right training for you.

Request For Call Back

020 7117 2515